1/2022

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

45. Jahrgang
ISSN 0137-7767
14,00 Euro



■ Digitalisierung und Datenschutzpolitik im Bund – bis 2025 ■ Die Institutionalisierung der Datenschutzkonferenz im BDSG ■ Theorie und Praxis der Bestandsdatenauskunft am Beispiel von E-Mail-Diensten ■ Zeigt Telegram, dass das Internet immer noch ein rechtsfreier Raum ist? ■ Digitalisierung und Datenschutz im Koalitionsvertrag 2021-2025 der Parteien SPD, Bündnis 90/Die Grünen, FDP ■ Pressemitteilungen ■ Nachrichten ■ Rechtsprechung ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine

Dienstag, 05.04.2022,
Datenschutz-Fachtag Kommunales Bildungswerk,
Berlin oder virtuell

Dienstag-Donnerstag, 26.-28.04.2022,
FFD-Datenschutztage,
Wiesbaden oder virtuell

Freitag, 29.04.2022,
Verleihung der BigBrotherAwards,
Bielefeld

Samstag, 30.04.2022,
DVD-Vorstandssitzung,
Bielefeld

Sonntag, 01.05.2022,
Redaktionsschluss DANA 2/2022,
Schwerpunkt: Social Media

Dienstag/Mittwoch, 10./11.05.2022
BvD-Verbandstage 2022
Berlin

Donnerstag/Freitag, 12./13.05.2022,
Fachtagung Datenschutz im Gesundheitswesen, GMDS u.a.,
Berlin

Montag/Dienstag, 20./21.06.2022,
DuD 2022 - Datenschutz und Datensicherheit, Jahresfachkonferenz, Computas,
Berlin

Montag, 12.09.2021,
Sommerakademie des Unabhängigen Landeszentrums für Datenschutz,
Kiel

Foto: Pixabay..com

DANA
Datenschutz Nachrichten
ISSN 0137-7767
45. Jahrgang, Heft 1

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Dr. Thilo Weichert
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autorinnen und Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Dr.-Mack-Straße 83
90762 Fürth
www.onlineprinters.de
Tel. +49 (0) 9161 6209800
Fax +49 (0) 9161 8989 2000

Bezugspreis
Einzelheft 14 Euro. Jahresabonnement 48 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Nach einem Jahr kann das Abonnement jederzeit mit einer Frist von einem Monat gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, Pixabay, iStock,
Titel: iStock/MarioGuti/venakr,
Wikimedia

Editorial


Bild: iStock | MarioGuti

Das letzte DANA-Heft widmete sich den Erwartungen an die neue deutsche Datenschutzpolitik. Das Heft 1/2022 hat die Versprechungen zum Thema, die jetzt gemacht werden. Ob dann „geliefert“ wird, werden wir in den nächsten 3 ½ Jahren sehen – mehr Zeit bleibt nicht mehr. Um die Versprechungen sofort griffbereit zu haben, wenn es mit der „Lieferung“ hapert, dokumentiert das Heft die relevanten Passagen des Koalitionsvertrags der rot-grün-gelben Koalition. Eine Analyse des Koalitionsvertrags begründet in Sachen Datenschutz ein wenig Optimismus, ist dann aber angesichts vieler Lücken und Fragezeichen ernüchternd, wie Thilo Weichert aufzeigt. Die Ampel scheint willig zu sein, doch ist ein Plan noch nicht so richtig zu erkennen. Ein Beispiel hierfür ist die bisherige föderale Datenschutzorganisation, der sich Markus Schröder widmet. NGOs wie die Deutsche Vereinigung für Datenschutz haben die wichtige Funktion beim Liefern nachzuhelfen – durch die Politik anregende Initiativen und, wenn nötig, kritische Kommentare.

Den Niederungen der konkreten Umsetzung von Digitalpolitik widmen sich Elias Zimmermann in Bezug auf die sicherheitsrechtlich motivierten Bestandsdatenauskunftsersuchen und Klaus-Jürgen Roth in Bezug die Einhegung von Telegram, wo sich allzu viele Idioten, Hetzer und Kriminelle tummeln. Eine Darstellung landesverfassungsrechtlicher Rechtsprechung im Sicherheitsbereich durch Arnold von Bosse rundet den redaktionellen Teil des vorliegenden Heftes ab.

Für Viele ist die DANA wichtig, weil sie eine Fundgrube für Meldungen über Entwicklungen und Fakten aus Deutschland und der ganzen Welt ist. Die DANA hat es sich zur Aufgabe gemacht insofern verlässliche Informationen aus den Tagesmedien und von der Gerichtsbarkeit aufgearbeitet zur Verfügung zu stellen.

Die DVD als NGO sieht (vor allen Dingen auch mit der DANA) einen Auftrag darin die Szene der Datenschützerinnen und Datenschützer in Stadt und Land nicht nur zu bereichern und zu unterstützen, sondern diesen auch Motivator und Sprachrohr zu sein. Insofern mögen sich die Lesenden auch zum Schreiben angeregt sehen: Das nächste Heft hat als Schwerpunkt „Social Media“. Wer hierzu etwas Wichtiges beitragen möchte, ist eingeladen uns dies mitzuteilen bis zum nächsten Redaktionsschluss am 1. Mai 2022. Auch Reaktionen auf unsere bisherigen Publikationen sind natürlich herzlich willkommen.

Eure bzw. Ihre DANA-Redaktion

Autorinnen und Autoren dieser Ausgabe:

Dr. Arnold von Bosse, Rechtsanwalt, Stralsund, a.v.b@in-mv.de

Klaus-Jürgen Roth, Bonn, dvd@datenschutzverein.de

Markus Schröder, LL.M., Rechtsanwalt und Lehrbeauftragter für IT-Recht an der Hochschule Heilbronn, markus.schroeder@hs-heilbronn.de

Dr. Thilo Weichert, Vorstandsmitglied der DVD,
Netzwerk Datenschutzexpertise, Kiel, weichert@datenschutzverein.de

Elias Zimmermann, Mitglied der DVD, elias_zimmermann@posteo.de

Thilo Weichert

Digitalisierung und Datenschutzpolitik im Bund – bis 2025

Neuanfang

Nach 16 Jahren *CDU/CSU-dominierter Bundespolitik* steht Deutschland mit der neuen Rot-grün-gelben Mehrheit im Bundestag und einer von der Ampelkoalition getragenen Regierung an einem Neuanfang – in fast allen Politikbereichen. Dies gilt auch für den Datenschutz und die damit eng zusammenhängende Digitalisierungspolitik. In den letzten 16 Jahren kamen von der Bundespolitik beim Datenschutz sowie generell zugunsten eines digitalen Grundrechtsschutzes keine neuen Impulse. Es wurden den Initiativen Europas und – so selten diese waren – des Bundesrates ausgebremst, wenn damit zwecks Schutz der informationellen Selbstbestimmung Zumutungen für die Verwaltung oder die Wirtschaft verbunden gewesen wären. In deren Interesse wurden Schutzmechanismen geschleift. Für den Datenschutz erfolgten keine signifikanten Investitionen. Datenschutz eignete sich vor allem als Prügelknabe für verpasste Digitalisierungschancen, unterbliebene Innovation, administrative Untätigkeit und illegale Cyberaktivitäten.

So liegen nun viele Erwartungen auf den Schultern der *neuen Regierung* und den neuen parlamentarischen Mehrheiten. Die Rahmenbedingungen sind auch ermutigend: die Politik ist jünger, diverser, grundrechts- und werteorientierter, digital kompetenter und sozialer als zuvor.[1] Dies begründet Hoffnungen für die nächsten vier Jahre Bundespolitik. Doch diese Hoffnung besteht nicht nur hinsichtlich des Datenschutzes, sondern in fast allen Lebensbereichen, so dass schon ein übergeordneter Blick ernüchtert: Geht es nach der SPD, so steht soziale Gerechtigkeit im Vordergrund; bei den Grünen sind dies Ökologie und Klimaschutz; und der FDP geht es um die Wahrung der Privilegien der ökonomischen Elite. Datenschutz ist für keine der Parteien ein Topthema.

Dass v.a. *FDP und Grüne* im Wahlkampf „Digitalisierung“ als Buzzword nutzten, muss für den digitalen Grundrechtsschutz noch nichts bedeuten: Die Erinnerung ist noch lebendig an das FDP-Motto aus 2017 „Digitalisierung first – Bedenken second“. Wen anderes als den Datenschutz meinte die FDP, wenn sie Bedenken zurückstellen wollte? Wenig ermutigend ist auch ein Blick auf die Regierungspolitik in den Bundesländern, wo die Grünen oder die FDP vertreten waren oder sind. Datenschutz spielte und spielt dort keine oder nur eine untergeordnete Rolle, so etwa mit grüner Beteiligung in Hessen und Baden-Württemberg oder mit den Liberalen in Nordrhein-Westfalen. In Sachsen-Anhalt wurde mit grüner Regierungsbeteiligung der Datenschutz rechtlich und personell über Jahre hinweg untergebuttert.[2] Zwar gab es die eine oder andere positive Initiative, etwa über die Blockadeposition der Grünen im Bundesrat, doch wurde diese nur sehr zurückhaltend beim Datenschutz eingesetzt.

Koalitionsvereinbarung generell

Für die Koalitionsvereinbarung der Ampel sind die Themen nun relevant: „Digital“ kommt dort – in verschiedenen Variationen – 188-mal vor, „Datenschutz“ immerhin 13-mal. Doch ist die Suche nach einem grundrechtsbasierten Digitalisierungs- oder einem Datenschutzkonzept wenig ergiebig. In vielen Passagen der Vereinbarung finden sich Schnipsel, die hierzu einen Beitrag leisten können. Und es steht nichts im Koalitionsvertrag, was zu einer digitalen Grundrechtspolitik in einem klaren Widerspruch stünde. Aber von einem Konzept kann keine Rede sein. Dies ist nicht nur darauf zurückzuführen, dass die Koalitionsvereinbarung ein Kompromiss ist und in Eile zusammengeschrieben werden musste. Diese *Konzeptionslosigkeit* liegt auch daran, dass keiner der drei Partner wirklich ein Konzept für einen digitalen Grundrechtsschutz hat. Zwar haben es die Begriffe „digitale Bürgerrechte“ (S. 16) sowie „Internetfreiheit und digitale Menschenrechte“ (S. 147) in das Koalitionspapier geschafft. Doch scheint vergessen, dass Vertreter aller an der aktuellen Regierung beteiligten Parteien gemeinsam den Entwurf einer europäischen Digitalen Grundrechte-Charta verantworteten.[3]

Komplexer digitaler Grundrechtsschutz

Das Problem bei der Erarbeitung eines Konzeptes eines digitalen Grundrechtsschutzes besteht darin, dass dieses aus einer *Vielzahl von Elementen* bestehen muss. Es geht nicht nur um „informationelle Selbstbestimmung“ im Sinne der Volkszählungsentscheidung des Bundesverfassungsgerichts aus dem Jahr 1983[4], sondern auch um Verbraucherschutz, Datensicherheit, Wettbewerbsregulierung, Verteidigung der digitalen Meinungsfreiheit, Beschäftigtenrechte, Minderheitenschutz, demokratische Transparenz, Kriminalitätsbekämpfung. Es geht oft zugleich um Datennutzung und Datenschutz, so etwa bei der Forschung, vor allem im Medizinbereich, bei der Informationsfreiheit im Interesse administrativer und wirtschaftlicher Kontrollierbarkeit, oder bei der Statistik im Interesse politischer Planung. Und jede der Grundrechtsanliegen, zu denen es jeweils einen umfangreichen Gesetzesrahmen gibt, hat nicht nur eine nationale, sondern auch eine europäische und oft sogar eine globale Dimension.

Auch die *Organisation des digitalen Grundrechtsschutzes* ist komplex. Es gibt da die unabhängigen Datenschutzbeauftragten. Diese sind Mosaiksteine eines größeren, teils noch sehr heterogen erscheinenden Ensembles.[5] Diese Gesamtheit enthält Teile, die dem Daten-

schutz nahe stehen, etwa die Verbraucherschutzorganisationen oder die Arbeitnehmervertretungen. Dann gibt es Stellen mit geringen organisatorischen Überschneidungen zum Datenschutz, bei denen aber eine größere Nähe wünschenswert ist, etwa das Bundesamt für die Sicherheit in der Informationstechnik (BSI). Marktregulierungs- und Wettbewerbsbehörden auf Bundes- und Europaebene beginnen derzeit den Verbraucher- und den Datenschutz zu entdecken. Wenig im Blickfeld steht bisher die Medienaufsicht, die das Anliegen der Meinungsfreiheit, des Jugendschutzes und des demokratischen Diskurses mit Digitalmedien verfolgt. Ins Gesamtbild gehören zudem die Behörden der Strafverfolgung und Gefahrenabwehr, die gefordert sind, wenn es um kurzfristiges Eingreifen oder um das Sanktionieren wegen Verstößen gegen den Datenschutz, das allgemeine Persönlichkeitsrecht oder sonstige Grundrechte geht. Bei Polizei und Staatsanwaltschaften, die durchsuchen, beschlagnahmen, vernehmen, fahnden und verhaften (lassen), liegen Grundrechtsschutz und Grundrechtseingriffe nahe beieinander.

Diese Stellen in eine neue technik-, gesellschafts- und grundrechtsadäquate Ordnung zu bringen, ist eine schwierige Aufgabe. Angesichts möglicher Grundrechtskonkurrenzen bleibt es sinnvoll verschiedene Institutionen zu beauftragen, die ihre jeweilige spezifische Kompetenz zur Geltung bringen. Sie haben dabei sowohl eine gesellschaftliche als auch regelmäßig eine individualrechtsschützende Funktion. Um diese Aufgabe frei von sachfremden, z.B. partei- oder wirtschaftspolitischen Interessen wahrnehmen zu können, ist die rechtliche Absicherung einer *unabhängigen Aufgabenwahrnehmung* wichtig. Diese wird im Koalitionsvertrag dem Bundesamt für die Sicherheit in der Informationstechnik (BSI) zugesagt (S. 16). Der Europäische Gerichtshof (EuGH) hat eine größere Unabhängigkeit der Bundesnetzagentur eingefordert[6], dies zuvor auch schon für die Staatsanwaltschaften in Deutschland.[7] Zugleich muss aber auch eine hinreichende Kontrolle gewährleistet sein, was zum einen größtmögliche Transparenz wie auch die Einbindung in ein „Check and Balances“ erfordert. Sowohl hinsichtlich der Unabhängigkeit als auch der Transparenz bestehen Defizite, etwa beim BSI, das umfassend in die Dienst- und Rechtsaufsicht des Innenministeriums eingebunden ist, oder bei den Staatsanwaltschaften mit ihrer Einbindung in die Justizverwaltung.

Datenschutz national

Das Thema Datenschutz wird in der Koalitionsvereinbarung nicht in einem Kapitel, sondern in *unterschiedlichen Fachkapiteln* behandelt, die nicht aufeinander Bezug nehmen und die kein einheitliches Konzept erkennen lassen. Übergreifende Datenschutzthemen werden nicht, spezifische Fragestellungen werden selektiv behandelt. So wird die Stärkung des Bundesbeauftragten für den Datenschutz (BfDI) nur im Polizeikontext adressiert (S. 104). Die zentrale Frage, die für die Zukunft des Datenschutzes wesentlich ist, wie die Datenschutzaufsicht im föderalen Bundesstaat als Teil einer europäischen Struktur gestaltet werden soll, wird mit einem Satz abgehandelt (S. 17).[8]

Die Potenziale der Datenschutzzertifizierung und deren Förderung finden keine Erwähnung. Die große Koalition hat in Umsetzung der DSGVO ein Bundesdatenschutzgesetz (BDSG) in Kraft gesetzt, das in vieler Hinsicht die DSGVO konterkariert oder zumindest zu konterkarieren versucht. Ein Bekenntnis, dass diese Fehler bereinigt werden sollen, fehlt.[9]

Die Absicht ein *Beschäftigtendatenschutzgesetz* zu verabschieden, wird in einem Satz formuliert (S. 17). Der dazu eingerichtete Beirat beim Arbeitsministerium, der noch vor der Bundestagswahl im Sommer 2021 seine Empfehlungen veröffentlichen sollte[10], hat am 17.01.2022 seine Ergebnisse zur Verfügung gestellt.[11] Im Beirat hat sich die seit Jahrzehnten praktizierte Strategie der Arbeitgeberseite wieder bestätigt: Mitdiskutieren und Ergebnisse sabotieren. Ob diese Strategie auch bei der Ampel erfolgreich sein wird, hängt wohl vor allem von der Rolle der FDP ab, die Farbe bekennen muss, was ihr wichtiger ist: Unternehmensinteressen oder Bürgerrechte.

Verblüffend ist, dass das Thema *„IT-Sicherheit“* im gleichen Kapitel mit den Bürgerrechten behandelt wird. Diese Zuordnung ist zwar für Datenschützer nichts Neues, für die deutsche Politik wäre es dies aber wohl. Bisher wurde IT-Sicherheit eher als klassische Gefahrenabwehr in einem polizeilichen Sinne verstanden. „Security-by-design/default“ (S. 16) erinnert an die entsprechenden Privacy-Mechanismen. Dass ein defensiver Ansatz verfolgt wird und nicht ein aggressiver, wie wir ihn z.B. aus den US-amerikanischen IT-Sicherheitsstrategien kennen, zeigt sich darin, dass „Hackbacks“ als Mittel der Cyberabwehr abgelehnt werden (S. 16).

Die Überarbeitung des verfassungs- und europarechtswidrigen *Datenschutzes im Ausländerbereich* wird überhaupt nicht erwähnt, auch nicht im Kontext der Registermodernisierung die überfällige Reform des Ausländerzentralregisters.[12]

Sicherheitsrecht

In Bezug auf die „innere Sicherheit“ finden sich viele positive Ansätze. Dies beginnt mit der Etablierung von Polizeibeauftragten, der Einführung pseudonymer Kennzeichnungen von Polizistinnen und Polizisten und geht bis zum Ausbau der sicherheitsbehördlichen IT (S. 104). Unter der Überschrift „Freiheit und Sicherheit“ wird eine Evaluierung der Sicherheitsgesetze durch ein „unabhängiges Expertengremium (Freiheitskommission)“ angekündigt. Bis Ende 2023 soll dann eine vom Bundesverfassungsgericht geforderte Überwachungsgesamtrechnung[13] vorgelegt werden. Flächendeckende Videoüberwachung und der Einsatz von biometrischer Erfassung zu Überwachungszwecken werden abgelehnt. „Das Recht auf Anonymität sowohl im öffentlichen Raum als auch im Internet ist zu gewährleisten.“ Die Vorratsspeicherung soll „rechtssicher anlassbezogen“ geregelt werden[14]; mit der Login-Falle soll grundrechtsschonend ermittelt werden. Ermittlungszwecke rechtfertigen keine IT-Sicherheitslücken. Anders als in der Vergangenheit, als Sicherheitsgesetze immer wieder wegen Verfassungswidrigkeit überarbeitet werden mussten, sollen besondere Ermittlungsmaßnahmen wie z.B. die Quellen-TKÜ oder die Online-Untersuchung „nach den Vor-

gaben des Verfassungsgerichts" ausgestaltet werden (S. 108 f.). Dafür soll das Sicherheitsrecht generell umfassend reformiert werden (S. 110).

Die Bundesregierung stellt sich damit einer Mammutaufgabe. Das Sicherheitsrecht des Bundes umfasst die Normen für die Bundespolizei[15], das Bundeskriminalamt und die drei Bundesgeheimdienste sowie für weitere Einrichtungen wie u.a. das Zollkriminalamt, ZiTis. Hinzu kommt die Strafprozessordnung. Angesichts der hierzu vorhandenen detaillierten Verfassungsgerichtsrechtsprechung sind die inhaltlichen Vorgaben als äußerer Rahmen relativ klar konturiert. Doch hinsichtlich der politischen Spielräume besteht genügend Raum für politische Konflikte, etwa wenn es um eine verbesserte Kontrolle der Geheimdienste geht. Die zuständigen MinisterInnen, Marco Buschmann (FDP) und Nancy Faeser (SPD) dürften voll hinter den im Koalitionsvertrag verabredeten Zielen stehen. Es wird aber heftige Widerstände geben, nicht nur von der AfD und von CDU/CSU, sondern aus dem Apparat, aus den nachgeordneten Bundesbehörden wie aus den Ministerien selbst, insbesondere aus dem bisher durchgängig von der CDU/CSU bestimmten und personell besetzten Innenministerium.

Gespannt sein kann man bei der Geldwäschebekämpfung, wofür das FDP-geführte Finanzministerium den Hut auf hat (S.166). Dabei geht es nicht nur um die Behebung der Gesetzgebungsdefizite, sondern ebenso der Vollzugsmängel. Für diese Defizite war und ist der Datenschutz nicht verantwortlich. Die Statements der politisch Verantwortlichen hatten bisher mit der administrativen Praxis wenig gemein. Hier besteht die Chance eines hohen „Return of Investment", ebenso wie bei der Bekämpfung der Steuerkriminalität (S. 167). Zugleich ist hier die Unternehmenslobby besonders agil und war bisher erfolgreich. Diese Themen werden zu einer Nagelprobe, ob es die Ampel tatsächlich schafft, Deutschland vom Image einer Bananenrepublik zu befreien.

eGovernment

Hinsichtlich der Digitalisierung der Verwaltung sind positive Ansätze zu erkennen. Die Wirklichkeit ist noch weit von den politisch formulierten Ansprüchen entfernt. Die Behörden sollen die notwendige Technik erhalten; IT-Schnittstellen zwischen Bund und Ländern sollen etabliert werden (S. 12). Rechtlicher Ansatzpunkt im Bürgerkontakt soll das weiter zu entwickelnde Online-Zugangsgesetz (OZG) sein.[16] Mit dem *„Einer-für-alle-Prinzip"* (EfA, S. 15) digitalisiert jedes Land die Verwaltungsleistungen so, dass andere Länder sie nachnutzen können, dass sie also einen Onlineprozess nicht nochmal selbst entwickeln müssen. Digitale Antragsprozesse sollen nicht 16-mal in jedem Land und 11.000-mal in jeder Kommune einzeln entwickelt werden, sondern einmal, um Zeit, Ressourcen und Kosten zu sparen. Technisch setzt man auf „Open Source" und will sich so offenbar von der bisherigen Abhängigkeit von US-Konzernen, allen voran von Microsoft und Google, befreien. Dies gilt auch für die Cloud-Datenverarbeitung, für die eine sichere und transparente Verwaltungs-Cloud aufgebaut werden soll (S. 15).

Versprochen werden zudem ein „vertrauenswürdiges, allgemein anwendbares Identitätsmanagement sowie die verfassungsfeste *Registermodernisierung*" (S. 15). Modifikationen zu den bisherigen Reformplanungen sind nicht erkennbar. Zur Erhöhung der Bürgerfreundlichkeit soll das „Once-Only-Prinzip" etabliert werden (S. 32). Zur Identitätsklärung von Ausländern soll im Einzelfall die „Versicherung an Eides statt" genügen (S. 138). Digitale Vergabeverfahren für gefährdete Personen sollen eingeführt werden (S. 142). Dabei muss zwangsläufig das Ausländerzentralregistergesetz angefasst und geändert werden. Sollte es die Bundesregierung tatsächlich schaffen mit der Steuer-ID als Personenkennziffer und mit technischen Vorkehrungen einschließlich eines Datencockpits ein datenschutzkonformes Registermanagement zu etablieren, so wird dies ein Gewinn sein für Bürgerfreundlichkeit, Wirtschaftlichkeit und Datenschutz. Die Widerstände hierfür sind weniger politisch, sondern administrativ, bedingt durch knappe Finanzen, verteilte Zuständigkeiten, Technikferne und fehlende Innovationsbereitschaft der handelnden Personen.

Forschung

Durch bessere Rahmenbedingungen will die Ampel Hochschule, Wissenschaft und Forschung kreativer und wettbewerbsfähiger machen (S. 8). Geplant ist ein Aufbruch für die Forschung generell und für die Medizinforschung im Besonderen: Es sollen „Instrumente wie Datentreuhänder, Datendrehscheiben und Datenspenden" auf den Weg gebracht werden. „Ein Dateninstitut soll Datenverfügbarkeit und -standardisierung vorantreiben, Datentreuhändermodelle und Lizenzen etablieren" (S. 17). Die Koalitionäre wollen den Zugang zu Forschungsdaten für öffentliche und private Forschung mit einem „Forschungsdatengesetz umfassend verbessern sowie vereinfachen" und „Forschungsklauseln" einführen. Die nationale Forschungsdateninfrastruktur soll weiterentwickelt und ein europäischer Forschungsdatenraum vorangebracht werden. Dabei soll „Datenteilung von vollständig anonymisierten und nicht personenbezogenen Daten für Forschung im öffentlichen Interesse" ermöglicht werden (S. 21).

Gesundheit

In der Gesundheitswirtschaft will man die Potenziale der Digitalisierung nutzen, „um eine bessere Versorgungsqualität zu erreichen, aber auch Effizienzpotenziale zu heben" (S. 29). Die Stärkung der Digitalisierung im Gesundheitswesen soll u.a. über den Ausbau der gematik zu einer digitalen Gesundheitsagentur erreicht werden. Die Einführung der elektronischen Patientenakte (ePA) soll beschleunigt werden. Es wird versprochen: „Zudem bringen wir ein Registergesetz und ein Gesundheitsdatennutzungsgesetz zur besseren wissenschaftlichen Nutzung in Einklang mit der DSGVO auf den Weg und bauen eine dezentrale Forschungsdateninfrastruktur auf" (S. 83). Die Passagen zur Digitalisierung im Gesundheitsbereich lesen sich wie Verlautbarungen aus dem Hause Spahn, das sich nicht durch große Anwenderfreundlichkeit profiliert hatte.

Europa

Viele Digitalisierungskapitel im Koalitionsvertrag lassen erkennen, dass

sie auch eine europäische Dimension haben, die *durchgängig unterstützt* wird. Dies beginnt mit der Erwähnung der DSGVO als „gute internationale Standardsetzung". Es folgen positive Bewertungen von Digital Service Act (DSA, S. 17, 124), Digital Markets Act (DMA, S. 19, 31, 124), der E-Privacy-Verordnung (S. 17)[17], der Verordnung zur „künstlichen Intelligenz" (AI-Act, S. 18), der Whistleblower-Richtlinie (S. 111), einer EU-Verbandsklagerichtlinie (S. 106), eines europäischen Gesundheitsdatenraums (S. 134 f.), der EU-Geldwäschebekämpfung (S. 171) und einer „Weiterentwicklung von Europol zu einem Europäischen Kriminalamt mit eigenen operativen Möglichkeiten" (S. 105). Weiter erwähnt werden die Förderung strategischer Technologiefelder z.B. im „Important Projects of Common European Interest" (IPCEI, S. 18), ein Europäischer Forschungsdatenraum (S. 21) und die Planung eines „digitalen Euros" (S. 172). Die europäische Cloud-Initiative Gaia-X wird nur als Basis einer europäischen Dateninfrastruktur in der Landwirtschaft adressiert (S. 47). Der nicht unwichtige Data Governance Act findet keine explizite Erwähnung. Bei der Plattformregulierung (Arbeitswelt, DSA, DMA) wird hervorgehoben, dass diese menschenzentriert und risikobasiert sein müsse (S. 72).[18]

Offenbar versteht die Koalition „eine konsistente EU-Digitalpolitik über Ressortgrenzen hinweg" als Weg zu europäischer *Souveränität* (S. 15, 16, 20, 132, 143, 144). Doch macht sie sich nicht soweit ehrlich, dass sie die Gegenspieler USA und China beim Namen nennt.

Informationsfreiheit und demokratische Transparenz

Die Koalition will „Transparenz und Teilhabe" in „einer unkomplizierten, schnellen und digitalen Verwaltung" realisieren (S. 8) und hierfür die Informationsfreiheitsgesetze zu einem *Bundestransparenzgesetz* weiterentwickeln (S. 11). Die Begriffe „digitale Teilhabe", „Barrierefreiheit" und „Netzneutralität" werden – ohne weitere Erläuterung – als Zielsetzungen genannt (S. 16).

Gespannt dürfen wir sein, wie weit die Ampelkoalition es mit den Anforderungen an die Transparenz gegenüber *privaten Playern* bringt. Die Absicht dafür besteht, etwa durch eine Ausweitung und Verbesserung des Lobbyregisters (S. 10) und des Transparenzregisters, mit dem wirtschaftlich Berechtigte öffentlich ausgewiesen werden (S. 172), und bei der Erhöhung der Transparenz beim Kredit-Scoring (S. 170). Da geht sicher noch mehr. Der Weg über Europa war in der Vergangenheit förderlich, etwa mit der Whistleblower-Richtlinie oder der geplanten KI-Richtlinie. Diese Initiativen waren von Deutschland bisher eher ausgebremst worden. Die Bundesregierung kann nun zum Antreiber werden.

Digitale Innovation

Unter dem Stichwort „digitale Schlüsseltechnologien" werden aktuelle Buzzwords aufgezählt: „Künstliche Intelligenz (KI), Quantentechnologien, Cybersicherheit, Distributed-Ledger-Technologie (DLT), Robotik". Insofern sollen *Investitionen gefördert* werden (S. 18). Im Kontrast zur bisherigen Regierungspolitik, die sich mit den Buzzwords schmückte, ohne dass viel passierte oder dass diese kritisch eingeordnet wurden, werden deren gesellschaftliche Funktionen und Risiken adressiert.

Resümee und Ausblick

In Sachen Digitalisierung kann sich der Koalitionsvertrag sehen lassen; in Sachen Datenschutz eigentlich auch, wenngleich insofern eher ein *Steinbruch* und nicht im Ansatz ein Konzept erkennbar ist. Angesichts dessen, dass sich hier drei politische Parteien mit teilweise stark voneinander abweichenden Selbstverständnissen einigen mussten, ist die vorliegende Vereinbarung beachtlich. Bei einem Jamaika-Bündnis wäre diese Detailliertheit nicht möglich gewesen.

Die Lücken, die es im Bereich Datenschutz gibt, können und müssen aufgefüllt werden. Ein Koalitionsvertrag beschreibt nicht abschließend, was eine Regierung in einer Legislaturperiode machen wird, sondern nur das, worauf sie sich zu Beginn der Zusammenarbeit geeinigt hat und was sie zu diesem Zeitpunkt als besonders wichtig einstufte. Neue Wichtigkeiten können sich ergeben; dies kann dadurch geschehen, dass *außerparlamentarisch Forderungen* an die Politik herangetragen werden. Angesichts der Grundeinstellungen, die die beteiligten Partner zu Digitalisierung und Datenschutz haben sind insofern keine allzu großen Meinungsunterschiede zu erwarten.

Die Umsetzungshindernisse haben sich nur wenig gegenüber denen der vorigen Legislatur verändert: Im Grunde sind alle Ressorts von der Digitalisierung und dem Datenschutz betroffen. Verkehrsminister Volker Wissing trägt die Zuständigkeit für Digitales im Namen seines Aufgabenbereichs, doch liegen die Fragen der rechtlichen Umsetzung eher beim Innen- und beim Justizministerium. Die Umsetzung liegt bei allen Ressorts, vor allem beim Innenministerium. In der letzten Legislaturperiode überboten sich die Ressorts in wolkiger, teils profilierungssüchtiger Rhetorik. Sie bekämpften sich oft mehr, als dass sie zusammenarbeiteten. Insofern lassen das nun handelnde Personal und die zu Beginn der Kooperation versendeten Botschaften mehr Seriosität und *mehr gemeinsames Handeln* erwarten. Luftnummern à la Lufttaxis einer Dorothea Bär zeichnen sich bisher eher nicht ab.

Konsistente übergreifende Strategien sind bisher aber nicht erkennbar. In vielen Themenbereichen bedürfte es einer *Koordination*. Diese sollte in kleinen handlungsfähigen zumeist ressortübergreifenden Arbeitsgruppen erfolgen, die dabei die in der Zivilgesellschaft, der Wirtschaft und der Wissenschaft vorhandenen Kompetenzen bündeln und in konkrete Initiativen lenken. Wenig optimistisch stimmt, dass im Bereich Digitalisierung das Kanzleramt und Bundeskanzler Olaf Scholz keine eigenen Zuständigkeiten sehen. Hier fordert bzw. „bestellt" der Koalitionsvertrag Führung, ohne dass sie – soweit erkennbar – bisher geliefert wird.

Bevor es zur Koordination der Ausführung kommt, muss die Koalition zunächst klären, welche Ressorts für welche Planungen überhaupt zuständig sein sollen. Dies lässt sich aus dem Ampelvertrag nicht ableiten und ist bei vielen Projekten, etwa dem zu einem „Dateninstitut" (S. 17), völlig unklar. Hierüber haben sich wohl die Verhandelnden auch noch keine konkreten Ge-

danken gemacht. Es ist im Interesse der Umsetzung der Vereinbarung wie der Transparenz für alle Beteiligten, dass eine ressortübergreifende Arbeitsgruppe sich über Betroffenheiten, *Zuständigkeiten und Hausaufgaben* verständigt und diese öffentlich macht. Es wäre nicht nur, aber auch für die Ampel fatal, wenn nach 4 Jahren festgestellt werden müsste, dass viele Absichtserklärungen in dem Vertrag nichts Anderes waren als ein unverbindliches Wünsch-dir-was.

Größtmögliche *Transparenz bei den Verfahren* ist wünschenswert. In der EU ist es gängige Praxis, dass Initiativen öffentlich zur Debatte gestellt werden. In Deutschland muss eine solche Praxis erst noch etabliert werden. In der Vergangenheit wurden oft teure Anwaltskanzleien mit der Projektentwicklung beauftragt, die regelmäßig einseitig Wirtschaftsinteressen umsetzten. Zukünftig sollten ein breiteres Lobbyspektrum und die Zivilgesellschaft einbezogen werden.

Die *Zivilgesellschaft* ist gefordert, Kontakt zu den zuständigen Parlamentariern und den Ministerialen aufzubauen, die mit digitalem Grundrechtsschutz zu tun haben. Die Verweigerungshaltung, die die große Koalition und deren Administration zeigte, sollte sich nicht reproduzieren. Dabei haben sich einige Rollen verändert: War es bisher möglich Anfragen und sonstige Transparenzinitiativen über die Grünen und die FDP zu starten, so sind deren Parlamentarier nunmehr gezwungen zumindest Rücksicht auf die Regierungspolitik und die Ministerialverwaltung zu nehmen. AfD und CDU/CSU hierfür zu instrumentalisieren dürfte wenig erfolgversprechend sein. Umso begrüßenswerter ist es, dass die Linken weiterhin im Parlament vertreten sind und für Themen des digitalen Grundrechtsschutzes ein offenes Ohr und zudem kompetente Politikerinnen und Politiker haben. Wenn es aber um konkretes Regierungshandeln geht, muss der direkte Weg zu den zuständigen Ministerien oder über die Abgeordneten von SPD, Grüne und FDP gesucht und gefunden werden. Der Koalitionsvertrag bietet genügend Ansatzpunkte, um in den Bereichen Digitalisierung und Datenschutz als Türöffner genutzt zu werden.

1 Weichert, DANA 4/2021, 218.

2 Vgl. DANA 4/2019, 225; DANA 1/2019, 40; DANA 2/2018, 108 f.

3 https://digitalcharta.eu/

4 BVerfG 15.12.1983 – 1 BvR 209/83 u.a., NJW 1984, 419 ff.

5 Weichert, vorgänge 231/232 (3/4/2020), 147 ff.

6 EuGH 02.09.2021 – C-718/18.

7 EuGH 27.05.2019 – C-508/18, EuGH 24.11.2020 – C-510/19.

8 Siehe dazu den folgenden Beitrag von Schröder in diesem Heft.

9 Vgl. dazu die Erwartungen der DVD und des Netzwerks Datenschutzexpertise, DANA 4/2021, 232 f.

10 Vgl. https://www.denkfabrik-bmas.de/schwerpunkte/beschaeftigtendatenschutz/; DANA 3/2020, 183.

11 https://www.bmas.de/SharedDocs/Downloads/DE/Arbeitsrecht/ergebnisse-beirat-beschaeftigtendatenschutz.pdf;jsessionid=18A81C3B172CA1864C4F3F9D660CEE20.delivery2-replication?__blob=publicationFile&v=2.

12 Zu den Defiziten beim Ausländerzentralregister aktuell die Gesellschaft für Freiheitsrechte (GFF), in diesem Heft S. 16.

13 BVerfG 03.02.2010 – 1 BvR 256, 263 u. 586/08, Rn. 218, NJW 2010, 833; dazu Roßnagel, NJW 2010, 1238 ff.

14 Weichert, vorgänge 227 (3/2019), 59 ff., vgl. zivilgesellschaftlich Gruppen, DANA 4/2021, 233 f.

15 Zum Reformbedarf im Bundespolizeigesetz Arzt, ZRP 2021, 205 ff.

16 Warnecke, DANA 3/2021, 152 ff.; zur Fortentwicklung des OZG Guckelberger/Starosta, NVwZ 2021, 1161 ff.

17 Offener Brief von 13 NGO, DANA 4/2021, 235 ff.

18 Zum europäischen Datenraum Roßnagel, ZRP 2021,173 ff.

Markus Schröder, LL.M.

Die Institutionalisierung der Datenschutzkonferenz im BDSG

Einleitung

Die Datenschutzkonferenz (DSK) ist nach der Definition in ihrer Geschäftsordnung der Zusammenschluss der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder und besteht aus der oder dem Bundesbeauftragten für den Datenschutz, den Landesbeauftragten für den Datenschutz und der Präsidentin oder dem Präsidenten des Bayerischen Landesamtes für Datenschutzaufsicht.[1] Ihre Aufgabe ist es sich mittels Entschließungen, Beschlüssen, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen auf gemeinsame Positionen der Datenschutzaufsichtsbehörden des Bundes und der Länder zu verständigen.[2] Ihre Tätigkeit steht dabei in einem Spannungsverhältnis zur Tätigkeit des Europäischen Datenschutzausschusses (EDSA), dessen Tätigkeit in Art. 68 ff. DSGVO geregelt ist. Die Tätigkeit der DSK ist demgegenüber nicht gesetzlich geregelt, sondern lediglich in der ihr selbst gegebenen Geschäftsordnung.[3] Aus Sicht der Verantwortlichen ist daher insb. aus zwei Gründen Rechtsunsicherheit entstanden: Zunächst stellt sich die Frage der Verbindlichkeit von Veröffentlichungen der DSK, falls diese

Fragen betreffen, die durch den EDSA noch nicht behandelt wurden. Zudem stellt sich die Frage der Verbindlichkeit der Veröffentlichungen auch für deren bundesweite Anwendung. So wurden verschiedene Veröffentlichungen nicht einstimmig angenommen. Beispielsweise wurde der Beschluss zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO auf ausdrücklichen Wunsch betroffener Personen gegen die Stimme Sachsens beschlossen.[4] Weiterhin wurde die Orientierungshilfe zu Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail gegen die Stimme Bayerns beschlossen.[5] Die neue Bundesregierung hat die Absicht, diese Rechtsunsicherheit zu beenden, in den Koalitionsvertrag aufgenommen.[6] So soll zur besseren Durchsetzung und Kohärenz des Datenschutzes die Datenschutzkonferenz im BDSG institutionalisiert werden. Dabei sollen ihr, soweit rechtlich möglich, verbindliche Beschlüsse ermöglicht werden.

Aktuelle Rechtslage nach der Geschäftsordnung der DSK und nach dem BDSG

Zur Erreichung gemeinsamer Positionen strebt die DSK Einvernehmen an. Sofern kein Einvernehmen erzielt werden kann, soll die Entscheidung der Mehrheit anerkannt werden. Entschließungen, die sich auf einen Gegenstand beziehen, bei dem eine individuell-konkrete Betroffenheit eines Mitglieds besteht, dürfen nicht gegen die Stimme dieses Mitglieds verabschiedet werden. Bei Mehrheitsentscheidungen zu gemeinsamen Positionen werden auf Wunsch abweichende Voten durch die Bezeichnung des jeweiligen Mitglieds der DSK in dem zur Veröffentlichung bestimmten Dokument kenntlich gemacht.[7] Aus diesem Verfahren wird bereits deutlich, dass die Entschließungen der DSK keine Verbindlichkeit für Behörden entwickeln können und sollen, die bereits im Rahmen eines laufenden Verwaltungsverfahrens mit einem zu entscheidenden Sachverhalt befasst sind. Aber gerade bei den förmlichen Beschlüssen der DSK stellt sich die Frage nach deren Verbindlichkeit, da diese Positionen die Auslegung datenschutzrechtlicher Regelungen betreffen.[8] Verbindlichkeit gegenüber den Verantwortlichen stellt sich grundsätzlich erst durch einen durch die zuständige Behörde erlassenen Verwaltungsakt und die darin zum Ausdruck kommende Rechtsauffassung ein. Dies sind nach § 40 Abs. 1 BDSG die Aufsichtsbehörden der Länder sowie im Anwendungsbereich von § 9 Abs. 1 BDSG und § 29 TTDSG der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Eine Auflösung dieses Konflikts bieten auch die §§ 17 ff. BDSG nicht, da sie ausschließlich die Zusammenarbeit der Aufsichtsbehörden in Bezug auf den EDSA betreffen. Jedoch wird auch bereits an der Regelung in § 18 BDSG kritisiert, dass diese nicht zur Festlegung eines gemeinsamen Standpunktes geeignet ist und der Begriff des gemeinsamen Standpunktes nicht definiert wurde.[9] Auch ist das Verfahren zur Erreichung des gemeinsamen Standpunktes nicht hinreichend detailliert geregelt, da in § 18 Abs.1 Satz 3 BDSG nur gesagt wird, dass „zu diesem Zweck untereinander alle zweckdienlichen Informationen auszutauschen" sind. Falls kein Einvernehmen erzielt werden kann, greift das Verfahren zur Festlegung eines gemeinsamen Standpunkts nach § 18 Abs. 2 BDSG. Die genannten Bedenken bestehen auch hinsichtlich einer künftigen Regelung zu verbindlichen Beschlüssen der DSK.

Mögliche Rechtsnatur der Beschlüsse der DSK

Fraglich ist jedoch bereits grundsätzlich, ob Beschlüsse der DSK überhaupt Bindungswirkung entfalten können und was deren Rechtsnatur ist. Zunächst lässt sich an eine Selbstbindung der Verwaltung denken. Dabei hat im Sinne des Gleichbehandlungsgrundsatzes nach Art. 3 GG die Verwaltung ihr Ermessen in gleichgelagerten Fällen in gleicher Weise auszuüben. Die Selbstbindung der Verwaltung kann sich dabei aus einer existierenden Verwaltungspraxis ergeben. Dies wäre in den Fällen, die den Beschlüssen der DSK zu Grunde liegen, jedoch nicht der Fall. Diese Beschlüsse sind, wie gesehen, Positionen, die die Auslegung datenschutzrechtlicher Regelungen bzw. entsprechende Empfehlungen betreffen.[10] Damit entscheiden sie nicht bereits konkrete Fälle, sondern bereiten vielmehr abstrakt künftige Fallentscheidungen vor. Aus diesem Grund kann aber auch kein Verwaltungsakt nach § 35 Satz 1 VwVfG vorliegen. Eine Selbstbindung der Verwaltung kann weiterhin bereits durch veröffentlichte Verwaltungsanweisungen entstehen.[11] Als solche könnten die Beschlüsse der DSK durchaus angesehen werden. Bindungswirkung im Sinne einer Ermessensreduzierung auf null tritt hier bereits durch Veröffentlichung der Anweisungen ein.[12] In Bezug auf die Blacklists zu Datenschutz-Folgenabschätzungen nach Art. 35 Abs. 4 DSGVO wird außerdem diskutiert, ob es sich dabei um Allgemeinverfügungen nach § 35 Satz 2 VwVfG handeln könne.[13] Fraglich ist jedoch, ob eine Blacklist oder ein Beschluss der DSK eine Regelung i.S.v. § 35 Satz 2 VwVfG darstellt, da aus deren Veröffentlichung keine unmittelbare Verbindlichkeit folgt. Diese dürfte regelmäßig erst durch einen Verwaltungsakt der nach § 9 Abs. 1 BDSG bzw. nach § 40 Abs. 1 BDSG jeweils zuständigen Behörde geschehen. Vorzugswürdig für die weitere Betrachtung einer Verbindlichkeit von Beschlüssen der DSK ist somit die Selbstbindung der Verwaltung. Aber auch dabei ist zu berücksichtigen, dass diese Selbstbindung nur für Behörden im Rahmen ihrer jeweiligen Zuständigkeit eintreten kann. Zudem kann keine Bindung für die Behörden entstehen, gegen deren Stimme beschlossen wurde. Für Behörden außerhalb ihres Zuständigkeitsbereichs können die Beschlüsse der DSK schon deshalb keine Bindungswirkung entfalten, da diese für die umsetzenden Entscheidungen nicht zuständig wären. Für die Behörden, gegen deren Stimme die Beschlüsse gefasst wurden, können diese Beschlüsse keine Bindungswirkung entfalten, da diese Behörden zum Ausdruck gebracht haben, dass sie gerade nicht durch den entsprechenden Beschluss gebunden sein wollen. Die Fiktion einer Bindungswirkung durch einen Mehrheitsbeschluss der DSK dürfte ohne Änderung der abschließend formulierten Zuständigkeiten, jedenfalls bei der Annahme einer Selbstbindung der Verwaltung, schwer darstellbar sein. Daher sollte bei den Überlegungen zu

einer künftigen Institutionalisierung der DSK von den genannten Prämissen ausgegangen werden.

Vorschlag zu einer Institutionalisierung der DSK im BDSG

Die Zusammenarbeit der Aufsichtsbehörden in europäischen Angelegenheiten ist in § 18 BDSG geregelt. Eine Zusammenarbeit der Aufsichtsbehörden in nationalen Angelegenheiten könnte daher künftig in einem § 18a BDSG geregelt werden. In diese Regelung sollten möglichst detaillierte Regelungen zum Verfahren aufgenommen werden, um die Kritik an § 18 BDSG aufnehmen zu können. Dies müsste allerdings nicht im Gesetz selbst geschehen, sondern könnte durchaus auch durch einen Verweis auf die Geschäftsordnung der DSK erfolgen. Hierdurch ist einerseits gewährleistet, dass verbindliche Verfahrensregelungen bestehen. Andererseits können die Einzelheiten der Ausgestaltung aber auch auf die DSK selbst delegiert werden, um eine gewisse Flexibilität bei der Ausgestaltung zu ermöglichen. Weiterhin ist davon auszugehen, dass die Beschlüsse der DSK die Rechtsqualität einer Selbstbindung der Verwaltung haben. Schließlich ist zu berücksichtigen, dass lediglich in dem Bereich verbindliche Beschlüsse erfolgen können, in dem der EDSA noch nicht nach Art. 70 DSGVO tätig geworden ist. Vor diesem Hintergrund könnte eine Regelung zur Institutionalisierung der DSK im BDSG wie folgt aussehen:

„§ 18a Sonstiges Verfahren der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder

1. *Zur Erreichung des Ziels die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten, wird die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder eingerichtet.*
2. *Die Konferenz gibt sich eine Geschäftsordnung, in der das nähere Verfahren der Zusammenarbeit geregelt wird.*
3. *Die Konferenz erlässt Beschlüsse, die die Ermessensausübung der teilnehmenden Aufsichtsbehörden binden. Diese Bindungswirkung besteht nicht für Aufsichtsbehörden, gegen deren Stimme ein Beschluss gefasst wurde. Diese Bindungswirkung besteht nur für Aufsichtsbehörden im Rahmen ihrer jeweils gesetzlich geregelten Zuständigkeit.*
4. *Die Konferenz kann keine Beschlüsse zu Sachverhalten fassen, in denen der Europäischen Datenschutzausschuss bereits nach Artikel 70 der Verordnung (EU) 2016/679 tätig geworden ist."*

Fazit

Der Vorstoß der neuen Bundesregierung die DSK im BDSG zu institutionalisieren ist zur Schaffung von Rechtssicherheit begrüßenswert. Aber auch künftig dürfte die Rechtssicherheit begrenzt bleiben, da die Beschlüsse nur in einem eingeschränkten Umfang Bindungswirkung entfalten können. Dies ist nicht der Fall, falls der EDSA schon tätig wurde, falls der Beschluss gegen die Stimme einer Aufsichtsbehörde gefasst wurde oder falls eine zustimmende Behörde für eine konkrete Entscheidung zu dem durch die im Beschluss behandelten Sachverhalte nicht zuständig wäre. Ebenfalls können die weiteren Handlungsformen, neben den Beschlüssen, die in Punkt A.III. der Geschäftsordnung der DSK aufgeführt sind, keine Rechtsverbindlichkeit haben, die sie ihrer Natur nach schon durch Selbstbindung der Verwaltung darstellen können. Aber wenn zumindest, wie dargestellt, im Rahmen der Beschlüsse der DSK ein Mindestmaß an Rechtssicherheit für die Verantwortlichen hergestellt werden kann, wäre dies ein großer Fortschritt für eine einheitliche Anwendung der DSGVO.

1 Geschäftsordnung der DSK, A.I.

2 Geschäftsordnung der DSK, A.III.

3 Geschäftsordnung - Beschluss der DSK vom 05. September 2018 geändert durch Beschluss der DSK vom 29. September 2021, https://www.datenschutzkonferenz-online.de/media/dsk/Geschaeftsordnung_DSK_09-2021.pdf

4 Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 24. November 2021 - Zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO auf ausdrücklichen Wunsch betroffener Personen, Fn. 1, https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf

5 Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. Mai 2021 - Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, Fn. 1, https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf

6 Koalitionsvertrag zwischen SPD, Bündnis90/Die Grünen und FDP: Mehr Fortschritt wagen – Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, S. 17

7 Geschäftsordnung der DSK, A.IV.3.

8 Geschäftsordnung der DSK, A.III.

9 Sommer, in: Däubler / Wedde / Weichert / Sommer, EU-DSGVO und BDSG, 2. Aufl. 2020, § 18 BDSG Rn. 3 ff.

10 Geschäftsordnung der DSK, A.III.

11 BFH, Urteil vom 14.05.2009 - IV R 27/06

12 BFH, a.a.O., R. 23 ff.

13 Piltz/Lühe: DSFA-Blacklists nach Art. 35 Abs. 4 DS-GVO als Allgemeinverfügung? Verwaltungsrechtliche Einordnung und mögliche Rechtsschutzmöglichkeiten, RDV 2020, 65


Bild: Frans Valenta

Elias Zimmermann

Theorie und Praxis der Bestandsdatenauskunft am Beispiel von E-Mail-Diensten

Am 01.12.2021 ist eine Novelle des Telekommunikationsgesetzes (TKG) in Kraft getreten, welche E-Mail-Dienste unter anderem verpflichtet unter bestimmten Voraussetzungen staatlichen Stellen Auskunft über Bestandsdaten ihrer Kunden zu geben. Als Konsequenz eines Urteil des europäischen Gerichtshofs (EuGH) vom 13.06.2019[1] waren diese nicht mehr unter die Bestimmungen des Telekommunikationsgesetzes gefallen und daher zu solchen Auskünften auch nicht mehr verpflichtet gewesen. Dem hat der Gesetzgeber nun Rechnung getragen und den Anwendungsbereich des TKG so erweitert, dass er auch wieder E-Mail-Dienste umfasst. Dies gibt Anlass, einen kritischen Blick auf die Praxis der Bestandsdatenauskunft zu werfen, was am Beispiel des E-Mail-Dienstes Posteo geschehen soll, der seit 2014 jährliche Transparenzberichte veröffentlicht, die den Umgang des Unternehmens mit Auskunftsersuchen staatlicher Stellen ausführlich dokumentieren.

Rechtslage

Die sogenannte manuelle Bestandsdatenauskunft ist in § 174 des neu gefassten Telekommunikationsgesetzes geregelt. Eine Neufassung der entsprechenden Regelung (§ 113) des alten Telekommunikationsgesetzes war auch nötig geworden, da das Bundesverfassungsgericht die bisherige Vorschrift für verfassungswidrig erklärt hatte,[2] und war bereits am 02.04.2021 in Kraft getreten. Nach § 174 TKG sind bestimmte staatliche Stellen berechtigt von Telekommunikationsunternehmen unter gewissen Voraussetzungen Auskünfte über Bestandsdaten ihrer Kunden zu verlangen. Dazu gehören unter anderem die Strafverfolgungsbehörden, die Sicherheitsbehörden sowie die Nachrichtendienste. Unter Bestandsdaten versteht das Gesetz dabei Daten eines Endnutzers, die erforderlich sind für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste (§ 3 TKG). Im Fall von E-Mail-Diensten könnten dies etwa Anschrift, Telefonnummer, Alter oder Kontodaten eines Nutzers sein. Auskünfte über solche Bestandsdaten dürfen von den vorgenannten Behörden etwa zur Aufklärung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für gewichtige Rechtsgüter sowie zur nachrichtendienstlichen Vorfeldaufklärung verlangt werden. Im Gegensatz zur alten Regelung des Auskunftsverfahrens wurden die Voraussetzungen in der neuen Fassung wesentlich präziser gefasst.

Das Auskunftsverlangen muss im Regelfall schriftlich oder elektronisch unter Angabe der einschlägigen gesetzlichen Bestimmungen gestellt werden. Das war im Wesentlichen auch schon in der alten Fassung so geregelt. Gemäß dem Bundesdatenschutzgesetz (BDSG) und anderer datenschutzrechtlicher Bestimmungen müssen solche Anfragen dabei so ausgestaltet sein, dass die Vertraulichkeit personenbezogener Daten gewährleistet ist.

Missstände in der Praxis

Als einer von wenigen deutschen E-Mail-Diensten veröffentlicht das Unternehmen Posteo seit 2014 Transparenzberichte, welche alle behördlichen Anfragen zu Nutzerdaten, insbesondere Bestandsdaten, aber auch zu Inhaltsdaten und Verkehrsdaten, dokumentiert.[3] Obwohl Posteo seine Vertragsabschlüsse so gestaltet, dass gar keine Bestandsdaten erhoben werden und entsprechend auch keine weitergegeben werden können, geben diese Berichte einen höchst aufschlussreichen Einblick in die Praxis von Behörden bei Ersuchen um Bestandsdaten aus der Perspektive eines Unternehmens. Dabei zeigen sich erhebliche Mängel, was die Umsetzung der gesetzlichen Vorgaben anbelangt, sowohl hinsichtlich der sicheren Übertragung der Auskunftsersuchen als auch hinsichtlich ihrer Rechtmäßigkeit. So waren im Jahr 2018 von 28 Bestandsdatenersuchen nur 12 formal korrekt, im Jahr 2014 waren es von 17 sogar nur 2. In keinem Jahr war der Anteil nicht korrekter Bestandsdatenersuchen niedriger als ein Drittel. Bei den unzulässigen Ersuchen handelte es sich vielfach um Abfragen von Verkehrsdaten wie dynamischen IP-Adressen, die nicht unter die Kategorie der Bestandsdaten fallen und damit im Rahmen der Bestandsdatenauskunft nicht abgefragt werden dürfen. Darüber hinaus fehlte in vielen Ersuchen die vorgeschriebene Nennung der Rechtsgrundlage. Ein weiteres Problem ist die Übertragung der Auskunftsersuchen, welche häufig nicht im Einklang mit den datenschutzrechtlichen Vorgaben steht. So werden etwa Ersuchen unverschlüsselt übermittelt oder es werden nicht-dienstliche E-Mail-Postfächer für die Korrespondenz verwendet.

Reaktionen der Aufsichtsbehörden

Die Problematik der unsicheren Übertragung sensibler Daten bei behördlichen Bestandsdatenersuchen ist den Landesdatenschutzbeauftragten bewusst, wie Antworten auf Beschwerden zeigen, die Posteo im Rahmen seiner Transparenzberichte veröffentlicht. Hiernach wurden und werden die Behörden von den Datenschutzbeauftragten immer wieder auf die Notwendigkeit einer sicheren Übertragung derartiger Anfragen hingewiesen. Den Ausführungen der Datenschutzbeauftragten lässt sich allerdings auch entnehmen, dass sich ein entsprechendes Problembewusstsein bei den Behörden nur sehr mühsam erreichen lässt. Auf die viel-

fach unrechtmäßige Abfrage von Verkehrsdaten im Rahmen der Bestandsdatenauskunft wurde der Rechtsausschuss des deutschen Bundestags bereits 2012 durch eine Stellungnahme des Bundesverbands der Informationswirtschaft (BITKOM) aufmerksam gemacht.[4] Die hierzu befragte Bundesregierung hielt indes die Vorwürfe für unbegründet und sah dementsprechend keinen Handlungsbedarf. Dabei begnügte sie sich mit der Befragung verschiedener Ermittlungsbehörden zu diesem Vorwurf, ohne mit Unternehmen zu sprechen, die nach eigener Angabe solche Anfragen regelmäßig erhalten haben.[5] Im Jahr 2015 wiederholte die Bundesregierung diese Einschätzung und verwies dabei auch auf den Umstand, dass entsprechende Beanstandungen von Datenschutzkontrollinstanzen wie etwa den Datenschutzbeauftragten nicht vorlägen.[6] Wie allerdings verschiedene Antworten der Landesdatenschutzbeauftragten auf entsprechende Beschwerden von Posteo nahelegen, scheinen sich diese für die Problematik rechtswidriger Ersuchen nach Verkehrsdaten im Rahmen der Bestandsdatenauskunft gar nicht zuständig zu fühlen.

Lösungen?

Angesichts der offen zutage tretenden Missstände stellt sich die Frage, wie Theorie und Praxis der Bestandsdatenauskunft wieder besser zur Deckung gebracht werden können. Eine Option könnten zusätzliche rechtliche Kontrollmechanismen sein, wie sie durch den Richtervorbehalt bei eingriffsintensiveren Maßnahmen wie etwa der Telekommunikationsüberwachung (TKÜ) grundsätzlich vorgesehen sind. Allerdings sind hinsichtlich der Wirksamkeit solcher Instrumente zur Begrenzung von Überwachungsmaßnahmen Zweifel angebracht, wie etwa Zahlen des Berliner Senats nahelegen, der sich seit 2004 von der Regierung Berlins über die Praxis der Telefonüberwachung in Berlin informieren lässt. Eine Auswertung der Jahresberichte von 2004 bis 2019 durch netzpolitik.org zeigte, dass seit 2007 kein einziger Antrag auf Überwachung mehr abgelehnt wurde.[7] Bereits im Jahr 2003 kamen Studien der Universität Bielefeld sowie des Max-Planck-Instituts für ausländisches und internationales Strafrecht zu dem Ergebnis, dass die Praxis der richterlichen Überprüfung von Überwachungsmaßnahmen gravierende Missstände aufweist und kaum Kontrollwirkung entfaltet.[8] Ein Grund hierfür mag in der hohen Zahl an beantragten Überwachungsmaßnahmen bei gleichzeitig schlechter personeller Ausstattung der Gerichte liegen. Umso fraglicher erscheint es, dass rechtliche Kontrollinstrumente, die bereits bei einem wesentlich intensiveren Eingriff wie der TKÜ ihrer Aufgabe nicht gerecht werden, zu einer rechtlichen Einhegung und Begrenzung bei der Bestandsdatenauskunft führen würden. Deren Praxis hängt auch wesentlich davon ab, wie (un)genau Unternehmen Auskunftsersuchen von Behörden prüfen und wie (un)kritisch sie diesen nachkommen. Zu einem kritischen Blick können sie letztlich nur dadurch bewegt werden, dass Kunden den Schutz ihrer persönlichen Daten ernst nehmen und diesen auch aktiv einfordern.

1 EuGH, 13. 6. 2019 - C-193/18.

2 BVerfG, 27. 5. 2020 - 1 BvR 1873/13, 1 BvR 2618/13.

3 Abrufbar unter https://posteo.de/site/transparenzbericht.

4 Siehe https://www.bitkom.org/Bitkom/Publikationen/Entwurf-eines-Gesetzes-zur-Aenderung-des-TKG-sowie-zur-Neuregelung-der-Bestandsdatenauskunft.html.

5 Deutscher Bundestag, Drucksache 17/12239, https://dserver.bundestag.de/btd/17/122/1712239.pdf.

6 Deutscher Bundestag, Drucksache 18/5804, https://dserver.bundestag.de/btd/18/058/1805804.pdf.

7 https://netzpolitik.org/2020/telefonueberwachung-2019-in-berlin-wurde-seit-zwoelf-jahren-kein-antrag-auf-ueberwachung-von-telefon-oder-internet-abgelehnt/.

8 O. Backes, C. Gusy: Wer kontrolliert die Telefonüberwachung? Eine empirische Untersuchung zum Richtervorbehalt bei der Telefonüberwachung. Bielefelder Rechtsstudien Band 17, Frankfurt, 2003 sowie H.-J. Albrecht, C. Dorsch, C. Krüpe: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen. Forschung aktuell Nr. 17. Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg i. Br. 2003.

Klaus-Jürgen Roth

Zeigt Telegram, dass das Internet immer noch ein rechtsfreier Raum ist? (Ein Kommentar)

Unsere Hoffnung in den 90er Jahren, die von vielen Bürgerrechtsbewegten und Digitalaffinen geteilt wurde, war, dass das Internet ein Hort der Informationsfreiheit und der offenen demokratischen Diskussion sein wird. Diese Hoffnung hat sich nur teilweise erfüllt. Wir haben die Rechnung nicht mit den IT-Konzernen, Demokratiefeinden und Cyberkriminellen gemacht. Durch sie ist das Internet auch zu einem Hort von Kriminalität geworden sowie von Hass, Hetze und Falschnachrichten. Dies schädigt die Gesellschaft, beeinträchtigt die demokratische Meinungsbildung und treibt die Menschen auseinander. Auch die Persönlichkeitsrechte vieler Menschen und der Datenschutz werden hierüber beeinträchtigt.

Das Internet war nie ein rechtsfreier Raum. Doch hinkt die Regulierung und



Bild: iStock | stockcam

deren Durchsetzung oft weit hinter der Realität hinterher. IT-Konzerne und Cyberkriminelle finden immer wieder Wege, wie sie zu ihrem Nutzen sanktionsfrei die Rechte Anderer im Netz verletzen können. Die „Flucht ins Ausland" ist dabei seit Jahrzehnten ein Klassiker, den auch Telegram praktiziert und damit Bösewichten eine Plattform bietet – zu deren und zu Telegrams Vorteil.

Telegram ist zwar ursprünglich als Messenger gestartet, aber durch neue Funktionen wie Gruppen mit bis zu 200.000 Mitgliedern und Kanäle, denen unbegrenzt viele Menschen folgen können und die öffentlich einsehbar sind, wird Telegram als soziales Netzwerk verwendet. Als solches fällt es unter das deutsche Netzwerkdurchsetzungsgesetz (NetzDG). Das heißt auch, dass Telegram eine Ansprechperson für die deutsche Justiz bereitstellen, einen einfachen Meldeweg für strafbare Inhalte einrichten und über diese Inhalte innerhalb von sieben Tagen eine Entscheidung treffen muss. Offensichtlich strafbare Inhalte müssten innerhalb von 24 Stunden gelöscht werden. Der Unterscheidung zu klassischen Messengern, auf die das NetzDG nicht anwendbar ist, liegt die Überlegung zugrunde, dass es sich bei sozialen Netzwerken um Werkzeuge der Massenkommunikation handelt, die Messenger dagegen der Individualkommunikation dienen.

Das Unternehmen selbst mit formalem Sitz in Dubai stellt sich quer und hat bisher alle Verfahren wegen Verstößen gegen das NetzDG sowie die massenhaften Anfragen des Bundeskriminalamtes (BKA) ignoriert. In seiner FAQ gibt Telegram auch an keine Löschanfragen zu privaten Konversationen und Gruppenchats zu beantworten. Das Unternehmen verfolgt explizit das Ziel den Usern eine Plattform an die Hand zu geben, die nicht von Regierungen kontrolliert werden kann. Dies ist in Diktaturen für die Opposition zweifellos ein Segen, doch in demokratischen Rechtsstaaten wird dies zur Katastrophe. Die Kanäle von Attila Hildmann hat das Unternehmen gelöscht; allerdings wird spekuliert, dass das erst auf Druck der App-Store-Anbieter Apple und Google hin geschehen ist.

Gegen Dienste wie Telegram gibt es so lange nur beschränkt wirksame Mittel, solange sich die beteiligten Staaten nicht auf gemeinsame Prinzipien bei der Bekämpfung von Kriminalität und gemeinschaftsschädlicher Nutzung des Internets verständigen. Diese Prinzipien sollten im besten Fall völkerrechtlich festgeschrieben und in internationaler Kooperation durchgesetzt werden. Davon sind wir aber noch weit entfernt, solange autoritäre Staaten wie z.B. China und Russland meinen, sie können daraus einen Nutzen ziehen, dass demokratische Gesellschaften durch Cyberattacken, Hatespeach und Fakenews destabilisiert werden. Diese „Logik" wird langfristig aber nicht verfangen. Daher sollten Bemühungen zur internationalen Kooperation bei der Bekämpfung nicht nur von klassischer Cyberkriminalität, also Online-Betrug, Identitätsdiebstahl, Ransomware-Attacken und Spionage, sondern auch vor Hass im Netz verstärkt werden. Es ist ein langer Weg, bis auch Staaten wie Dubai bzw. die Vereinigten Arabischen Emirate, wo sich offenbar Telegram versteckt, in eine globale Internetregulierung integriert sind.

Leider – und das gehört zum Thema – nutzen auch große Plattformanbieter Hass und Fakenews im Internet, um höhere Klickzahlen und längere Online-Zeiten der Nutzer zu produzieren. Die Whistleblowerin Francis Haugen hat dies bei Facebook bzw. Meta unwiderleglich offengelegt. Diese Hass- und Fake-Economy hat das Internet unfreier gemacht.

Kurzfristig muss gegenüber Telegram das Netzwerkdurchsetzungsgesetz angewandt werden. Telegram kann sich nicht darauf berufen als Messenger privilegiert zu sein. Nachdem seine Gründer angekündigt haben Werbung verkaufen zu wollen, liegt auch das Kriterium der Gewinnerzielungsabsicht vor. Das Bundesamt für Justiz hat daher zu Recht im Sommer 2021 zwei Verfahren gegen Telegram eingeleitet wegen Nichtdurchführung von NetzDG-konformer Moderation und wegen der Nichtbestellung eines in Deutschland ansässigen Zustellungsbevollmächtigten. Die Strafe kann bis zu 50 Millionen Euro betragen.

Sollte die Politik der Ansicht sein, dass der Wortlaut des NetzDG eine solche funktionsorientierte Betrachtung nicht hinreichend klar abbildet, so wäre es dem Gesetzgeber möglich dies kurzfristig durch ein Update des Gesetzes klarzustellen.

Die Plattform selbst darf aber nicht das einzige Ziel staatlicher Maßnahmen sein. Wenn es Hinweise auf Hass, Hetze und kriminelle Machenschaften gibt, müssen Sicherheitsbehörden die verwendeten Dienste für ihre Ermittlungsarbeit selbst nutzen und die konkreten Gesetzesverstöße sanktionieren.

Auch der Weg über die App-Stores von Google und Apple sollte zur Bekämpfung der Rechtsverstöße durch und von Telegram geprüft werden. Diese Gatekeeper können Telegram aus ihren App-Stores werfen, weil der Dienst Hass und Kriminalität eine Plattform bietet ohne zumutbare Sicherungsmechanismen zugunsten betroffener User einzuziehen. Solche Sicherungsmechanismen – etwa eine Reichweitenbeschränkung der Gruppen – wären denkbar und für den Anbieter technisch auch leicht umzusetzen.

Letztlich sind alle Messenger-User gefordert: Es ist offensichtlich, dass Telegram in Deutschland eine Plattform und ein Resonanzkörper auch für Kriminelle und Hetzer ist. Die User können durch ihr eigenes Kommunikationsverhalten dazu beitragen, dass Hass, Hetze und Aggressivität nicht toleriert werden. Es gibt seriösere Messenger, über die man sich verschlüsselt unbeobachtet und sicher austauschen kann – Signal, Threema oder Wire. Ein Umzug dorthin von Telegram trägt dazu bei, dass die Spreu vom Weizen getrennt wird.

Mittelfristig wird der Digital Service Act (DSA) europaweit koordinierte Aktivitäten ermöglichen. Mit dem DSA werden Plattformen künftig stärker in die Verantwortung genommen. Er wird auch Messengerdienste regulieren. Zwar fallen kleinere Dienste wie Telegram nicht unter die harten Moderations- und Transparenzpflichten wie Facebook, doch können nach dem Entwurf Gerichte und Behörden sehr wohl An-

ordnungen zur Beendigung von Rechtsverletzungen durch konkrete rechtsverletzende Inhalte treffen.

Es gilt das Marktortprinzip. Ausländische Unternehmen müssen sich an die europäischen Regeln halten, wenn sie ihr Angebot auf den europäischen Markt und auf Userinnen und User dort ausrichten. Mit dem DSA wird ein europäisch konzertiertes Vorgehen möglich sein. Die Erfahrungen mit Telegram eignen sich als Beispiel, um die Wirksamkeit der geplanten DSA-Maßnahmen zu überprüfen.

Arnold von Bosse

Handeln von Polizei und Verfassungsschutz in MV verfassungswidrig – Klage zur Internet-Bestandsdatenauskunft beim Landesverfassungsgericht MV erfolgreich

Besprechung zum Beschluss des Landesverfassungsgerichts Mecklenburg-Vorpommern v. 28.10.2021 – LVerfG 3/14

Das Landesverfassungsgericht Mecklenburg-Vorpommern hat am 28.10.2021 entschieden, dass die gesetzlichen Regelungen zur Bestandsdatenauskunft (abgerufen durch die Sicherheitsbehörden bei den Internet-Providern in strafrechtlichen Verdachtsfällen) in Mecklenburg-Vorpommern in relevanten Teilen verfassungswidrig sind.

Die vor allem von Mitgliedern der Partei Bündnis 90/Die Grünen erhobene Klage wurde in den Datenschutz Nachrichten 4/2014 besprochen (S. 162 ff.).

Der Entscheidung, der eine Abwägung von Datenschutz auf der einen und Sicherheitsinteressen auf der anderen Seite zugrunde liegt, ist nun – nach 7 Jahren Verfahrensdauer – zuzustimmen. Die aktuelle Praxis, nach der Polizei und Verfassungsschutz auch ohne das Vorliegen einer „konkreten Gefahr" Bestandsdaten wie Telefonnummern, Namen, Geburtsdaten und Adressen bei den Providern abfragen können, ist rechtswidrig und muss beendet werden.

Das Landesverfassungsschutzgesetz M-V und das Sicherheits- und Ordnungsgesetz M-V müssen nun vor diesem Hintergrund durch die Landesregierung novelliert werden, um die Grundrechte auf „informationelle Selbstbestimmung" (Art. 2 GG) und auf „Wahrung des Brief-, Post- und Fernmeldegeheimnisses" (Art. 10 GG) wieder zu gewährleisten.

§ 24b des Gesetzes über den Verfassungsschutz im Lande M-V und § 33h des Gesetzes über die öffentliche Sicherheit und Ordnung in M-V erlauben den Sicherheitsbehörden bei Telefon- und Internetprovidern Auskünfte zu Bestandsdaten einzuholen. Beide Normen sehen für die Einholung von Bestandsdatenauskünften aktuell nicht hinreichend begrenzende Eingriffsschwellen, wie zum Beispiel das Vorliegen einer „konkreten Gefahr", vor. Dies wurde vom Gericht als verfassungswidrig eingestuft.

Das Landesverfassungsgericht unterscheidet – so wie das in Bezug genommene Bundesverfassungsgericht mit Beschluss v. 27.5.2020, 1 BvR 1873/13 – zwischen der Übermittlung der Daten durch die Provider und dem Abruf der Daten durch die Verfassungsschutz- und Polizeibehörden (sog. Doppeltüren-Modell). Die Regelungen zum Abruf werden durch das Gericht kritisiert: Das Gericht prägt den Begriff der Notwendigkeit der „konkreten begrenzenden Eingriffsschwelle". Diese ist in den Gesetzen nicht deutlich genug normiert. Das Gericht spricht auch von der fehlenden „Normenklarheit" und dass die „Verhältnismäßigkeit" von Eingriff und Zweck nicht hinreichend gegeben sei.

Wie diese Regelungen konkret in den künftigen Gesetzen im Einzelnen ausformuliert werden müssen, überlässt das Gericht dem Landesgesetzgeber, da das Gericht nur den Rahmen und die Vorgaben gibt. Man hätte sich hier jedoch noch weitere Hinweise gewünscht, wie solche Schwellen aussehen sollten. Dies betrifft z.B. den zu fordernden Begriff der „Erforderlichkeit" anlässlich des Abrufes der Bestandsdaten.

Besonders widmet sich das Gericht den Bestandsdaten in den sog. dynamischen IP-Adressen (anhand der IP-Adressen können die Sicherheitsbehörden erkennen, wie der Verdächtige im Internet gesurft ist, d.h. welche Seiten er angeklickt hat). Dies lässt eine intensivere Sicht der Behörden auf persönliche Vorlieben zu, deren Vertraulichkeit besonders geschützt ist.

Daher fordert der Beschluss mit Recht die „Beschränkung auf Eingriffsbefugnisse" im Hinblick nur auf „Rechtsgüter von besonderem Gewicht". D.h., es müssen besonders gewichtige Rechtsgüter, wie z.B. das Leben von Personen, konkret gefährdet sein. Die bisherigen Regelungen verstoßen gegen das Grundrecht auf Entfaltung der Persönlichkeit in der Ausprägung des „Rechts auf informationelle Selbstbestimmung" (Art. 1 und 2 GG und die entsprechenden Landesverfassungsregelungen).

Die zum Abruf von sog. Zugangsdaten (Passwörter, PIN, PUK, Zugang zu E-Mail-Konten oder Cloud-Speichern) ermächtigenden § 24b (1) Satz 2 LVerfSchG und § 33h (1) Satz 2 SOG M-V werden im Beschluss dagegen als „für sich genommen hinreichend begrenzt und verhältnismäßig" angesehen. Eine Auskunft darf gemäß diesen Vorschrif-

ten nur verlangt werden, wenn „die gesetzlichen Voraussetzungen“ für die Nutzung der Daten vorliegen. Hier hätte man sich gewünscht, dass das Gericht verlangt hätte, dass konkret die einzelnen sog. „gesetzlichen Voraussetzungen“ zur Nutzungsberechtigung der Daten in den Normen zu nennen sind: Dies wäre ein Gebot der auch an anderer Stelle vom Gericht geforderten sog. Normenklarheit gewesen und wäre nicht nur für die Sicherheitsbehörden praxistauglicher.

Schließlich verlangt der Beschluss richtigerweise, dass bei der Verfolgung von Ordnungswidrigkeiten die Eingriffe und der Abruf der Daten nur bei „besonders gewichtigen Ordnungswidrigkeiten“ zulässig seien.

Dies und dass z.B. nur „Rechtsgüter von hervorgehobenem Gewicht“ tangiert sein dürfen, müssen die Sicherheitsbehörden schon ab Urteilsverkündung, also ab jetzt, berücksichtigen, obwohl der Landesgesetzgeber für die zu korrigierenden Gesetze noch bis zum 31.10.2022 Zeit hat. Insgesamt ist der Beschluss im Sinne des ausgewogenen Datenschutzes sehr zu begrüßen.

(Anmerkung: Der Autor hat anlässlich des Einlegens der Verfassungsbeschwerde diese in der DANA 4/2014, 162-164 dargestellt. Die Entscheidung des LVerfG M-V findet sich im Netz unter https://www.mv-justiz.de/static/MVJ/Gerichte/Landesverfassungsgericht/Entscheidungen/2021/LVerfG%203.14%20Beschluss%20anonym.pdf).

Presseerklärung der DVD vom 04.01.2022

DVD: „Impfregister ist datenschutzkonform möglich“


Bild: iStock | Leonsbox

Die Diskussion über eine Impfpflicht gegen Covid19 bzw. das Corona-Virus ist in vollem Gange. Klar ist dabei, dass eine solche generelle Impfpflicht der gesamten Bevölkerung nur über eine Corona-Impfregistrierung durchgesetzt und kontrolliert werden kann. Bundesjustizminister Marco Buschmann hat sich nun dazu geäußert und behauptet, dass Datenschützer gegen ein solches Impfregister seien. Damit reiht sich der Minister in eine lange Reihe von Politikern ein, die das Datenschutzargument vorschieben. Die Deutsche Vereinigung für Datenschutz e.V. (DVD) weist darauf hin, dass Datenschutz einer wirksamen Virusbekämpfung nie wirklich entgegenstand und dass Impfregister datenschutzkonform gestaltet werden können:

Der Aufbau einer Impfregistrierung bedarf, wie jede staatliche informationelle Maßnahme, einer gesetzlichen Grundlage, bei der die Eingriffe normenklar beschrieben und zugleich zur Wahrung der Verhältnismäßigkeit rechtliche Datenschutzvorkehrungen getroffen werden. Aus Sicht der DVD gibt es legitime Argumente für eine Impfregistrierung der Bevölkerung im Interesse der Gesundheit. Für die Rechtmäßigkeit eines solchen Vorhabens und auch um das Vertrauen der Bevölkerung zu gewährleisten, muss die Zweckbindung der Daten gewahrt werden. Dafür ist eine Etablierung dieser Registrierung in der Gesundheitsverwaltung sinnvoll. Diese sollte, um eine zu starke Zentralisierung zu vermeiden, bei den Landesgesundheitsämtern – mit einheitlicher Software – erfolgen, denen ein Austausch untereinander erlaubt wird, um Doppelerfassungen zu vermeiden. Durch eine Etablierung der Register bei den Landesgesundheitsämtern würde zudem die Kommunikation mit den örtlichen Gesundheitsämtern vereinfacht. Die Sanktionierung von Verstößen gegen eine mögliche Impfpflicht sollte der ärztlichen Fachverwaltung übertragen werden, die dem Patientengeheimnis unterliegt. Als Datengrundlage kann auf die Daten der Meldebehörden zurückgegriffen werden. Es sollte aber darauf geachtet werden, dass die sensiblen Gesundheitsdaten von der allgemeinen Ordnungsverwaltung und insbesondere der Polizei so weit wie möglich getrennt gehalten werden.

Bei einer Impfregistrierung sollte man sich nicht darauf beschränken lediglich den Impfstatus der Menschen zu erfassen. Sinnvoll ist auch die Speicherung von Arbeitsverhältnissen im Bereich kritischer Infrastrukturen, um im Bedarfsfall kurzfristig zusätzlich nötige Impfangebote organisieren zu können. Sinnvoll ist aus Sicht der DVD auch die Aufnahme von Angaben, mit denen die gesundheitlichen Folgen der Impfung sowie Erkrankungen, also Impfdurchbrüche, erfasst werden. Der Zugriff auf diese Daten muss aber der unabhängigen Forschung vorbehalten bleiben, die zur Wahrung eines Forschungsgeheimnisses rechtlich verpflichtet wird. Dadurch werden zeitnahe Aussagen über den Infektionsverlauf ermöglicht – woran es in Deutschland seit Ausbruch der Pandemie fehlt.

Thilo Weichert, DVD-Vorstandsmitglied und Experte im Bereich des Gesundheitsdatenschutzes, erläutert: „Gesundheitsschutz und Datenschutz dürfen nicht gegeneinander ausgespielt werden. Dies darf sich im dritten Coronajahr nicht fortsetzen. Omikron hat uns gezeigt, dass wir wohl mittelfristig mit dem Virus leben müssen. Dies bedeutet, dass schnell und grundrechtsschonend gehandelt werden muss. Dies ist durch die Digitalisierung der Gesundheitsverwaltung und durch eine grundrechtskonforme Gesetzgebung auch möglich. Es geht nicht darum ´Bedenken second´ zu behandeln. Gesund-

heitsschutz, Digitalisierung und Datenschutz passen – mit gutem Willen und klugem Handeln – gut zusammen."

Frank Spaeing, Vorsitzender der DVD, ergänzt: „Die oft in Debatten geäußerte Behauptung, der Datenschutz stünde (u.a.) der Pandemiebekämpfung im Wege, ist toxisch. Wir wünschen uns von der neuen Bundesregierung und den Koalitionspartnern, dass sie mit dieser unleidigen Tradition brechen. Datenschützer stehen im konkreten Fall den Gesundheitspolitikern gerne zum Dialog zur Verfügung."

Presseerklärung der Gesellschaft für Freiheitsrechte e.V. (GFF) vom 13.01.2022

GFF-Studie: Das Ausländerzentralregister verletzt Datenschutzstandards und die Grundrechte Millionen Betroffener

Zu viele Behörden können auf zu viele Daten für zu unterschiedliche Zwecke zugreifen – ohne ausreichende Kontrolle. Dies ist das Fazit der heute veröffentlichten Studie „Das Ausländerzentralregister – eine Datensammlung außer Kontrolle" der Gesellschaft für Freiheitsrechte e.V. (GFF).

Die Studie ergänzt ein von der GFF in Auftrag gegebenes, ausführliches Rechtsgutachten von Prof. Matthias Bäcker, das ebenfalls heute veröffentlicht wird. Es kommt zu dem Ergebnis, dass das Ausländerzentralregister (AZR) das Grundrecht auf informationelle Selbstbestimmung, das Diskriminierungsverbot sowie grundlegende europarechtliche Datenschutzstandards verletzt.

Mit etwa 26 Millionen personenbezogenen Datensätzen ist das Ausländerzentralregister eines der umfangreichsten automatisierten Register. Es steht mehr als 16.000 öffentlichen Stellen zur Verfügung. Die Studie der GFF untersucht, welche Daten aus ganz unterschiedlichen Lebensbereichen das AZR über Ausländer*innen in Deutschland speichert, wie diese Daten nahezu allen deutschen Behörden zugänglich sind und welche Schutz- und Kontrollmechanismen es auf dem Papier und in der Realität gibt.

Es ist rechtlich nichts dagegen einzuwenden, Grunddaten über Nicht-Deutsche zum Zwecke der Migrationsverwaltung zu speichern. „Das Ausländerzentralregister verletzt aber dort Grundrechte und Datenschutzstandards, wo unzählige weitere Datensätze



Bild: iStock | vichinterlang

gespeichert werden, die dann z.B. von Sicherheitsbehörden für völlig andere Zwecke genutzt werden können", sagt Sarah Lincoln, Juristin bei der GFF und Autorin der Studie. Besonders betroffen hiervon sind Geflüchtete, über die neben Grundpersonalien, Adresse, Foto und aufenthaltsrechtlichen Angaben auch biometrische Daten sowie Angaben zu Gesundheit, Bildung, Familie und Fluchtgründe gespeichert werden.

„Der Umfang der gespeicherten Daten ist unverhältnismäßig. Wofür soll es erforderlich sein, künftig sogar die Asylbescheide mitsamt hochsensiblen Angaben zu Flucht, psychischer Verfassung oder politischer Verfolgung zentral zu speichern und tausenden Behörden zugänglich zu machen?", fragt Lincoln.

Die Studie zeigt auch ein Folgeproblem dieser Datenfülle auf: „Wenn hunderttausende Mitarbeiter*innen von Ausländerbehörden, Polizei- und Strafverfolgungsbehörden, Nachrichtendiensten, Jobcenter, Jugendämtern und Gerichten auf so viele, teils hochsensible Daten zugreifen können, ist das Missbrauchspotenzial enorm", sagt Lincoln. „Im schlimmsten Fall geraten Daten wie Adresse, sexuelle Orientierung oder politische Überzeugung in die Hände von rassistisch motivierten Straftäter*innen oder Verfolgerstaaten und bringen Betroffene so in Lebensgefahr."

An der Studie wird deutlich, dass es an effektiven Kontrollmechanismen und Transparenz fehlt. Die GFF unterstützte 13 Betroffene dabei, Auskunft zu den über sie im AZR gespeicherten Daten zu beantragen und stellte fest: Das Antragsverfahren ist mühsam, die Antworten verzögerten sich monatelang und waren unvollständig.

Lincoln kritisiert die erhebliche Diskriminierung: „Eine derart umfangreiche Datensammlung über deutsche Staatsbürger*innen, auf die u.a. alle Polizeibehörden nach Belieben zugreifen können, wäre undenkbar. Bei Geflüchteten und anderen Migrant*innen setzt sich die Bundesregierung seit Jahren über geltendes Recht hinweg. Das wollen wir ändern. Gemeinsam mit Betroffenen planen wir strategische Klagen gegen die verfassungswidrigen Regelungen des Ausländerzentralregistergesetzes".

Weitere Informationen sowie die Studie und das Rechtsgutachten zum AZR finden Sie hier: https://freiheitsrechte.org/studie-azr

Bei Rückfragen wenden Sie sich an: Maria Scharlau, Pressesprecherin, Tel. 030/549 08 10 55; mobil 01579 2493108, Mail: presse@freiheitsrechte.org

Pressemitteilung von Digitalcourage vom 27.01.2022

Verwaltungsgericht hält Fingerabdruckpflicht für grundrechtswidrig


Bild: iStock | Fayethequeen

Ist die Speicherpflicht für Fingerabdrücke in Personalausweisen rechtmäßig? Diese Frage wird nun dem Europäischen Gerichtshof (EuGH) vorgelegt. Die Organisation Digitalcourage e.V., die sich für Grundrechte und Datenschutz einsetzt, hatte in erster Instanz gegen die Speicherpflicht geklagt. Das Verwaltungsgericht Wiesbaden folgt der Argumentation des Vereins und zweifelt die Rechtmäßigkeit der Fingerabdruckspflicht an. Da die deutsche Speicherpflicht auf einer EU-Verordnung basiert, muss nun der EuGH entscheiden.

Die Speicherpflicht gilt in Deutschland seit dem 2. August 2021. Seitdem müssen bei der Beantragung eines neuen Personalausweises die Fingerabdrücke beider Zeigefinger auf dem Chip des Ausweises gespeichert werden.

Nicht vereinbar mit europäischem Grundrecht auf den Schutz personenbezogener Daten

Die Speicherung von Fingerabdrücken wurde eingeführt, um eine angeblich bessere Fälschungssicherheit bei Personalausweisen zu erreichen. Digitalcourage zweifelt an, dass dieser Zweck überhaupt erfüllt wird. Denn eine Übereinstimmung der Fingerabdrücke einer Person mit den gespeicherten Abdrücken auf ihrem Ausweis macht lediglich klar, dass der Ausweis zur Person gehört. Die Echtheit des Ausweises – und damit die Identität der Person – beweist eine Übereinstimmung aber nicht. Die Speicherung der Fingerabdrücke auf dem Chip kann also höchstens für einige Zeit Fälschungen aufwendiger und teurer machen – bis professionelle Fälschungswerkstätten dementsprechend nachgerüstet haben. Dieser Vorsprung rechtfertigt aber auch nach Ansicht des Verwaltungsgerichtes nicht den schwerwiegenden Eingriff in die Grundrechte aller europäischen Bürger.innen.

„Wenn es zu einem Datenleck kommt, können wir unsere Passwörter ändern; wenn es sein muss auch die Handynummer. Wenn unsere biometrischen Daten in falsche Hände geraten, können wir dagegen nichts tun. Von einem Datenleck, das biometrische Informationen umfasst, wären wir unser ganzes Leben lang betroffen", sagt Julia Witte von Digitalcourage.

Dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) scheint der Ausweis auch ohne Fingerabdrücke schon sicher genug zu sein. Auf seiner Website erklärt das Amt, dass ein Ausweis auch gültig bleibe, wenn der Speicherchip defekt sei, denn „die Sicherheit als Ausweisdokument ist durch die physischen Sicherheitsmerkmale gegeben". Das wirft beim Verwaltungsgericht die Frage auf, warum die Fingerabdruckpflicht dann nötig sein soll. Auch die Anzahl der Fälschungen rechtfertigt die Maßnahme nicht, findet das Verwaltungsgericht Wiesbaden und zitiert eine Stellungnahme des Europäischen Datenschutzbeauftragten, die von 38.870 gefälschten Identitätskarten in den Jahren 2013–2017 spricht.

„Dieser verschwindend geringen Anzahl von Fälschungen gegenüber stehen 370 Mio. EU-Bürgerinnen und Bürger, deren intimste biometrische Informationen hier für ein Wettspiel zwischen Sicherheitsbehörden und Fälschungswerkstätten in den Ring geworfen werden", sagt padeluun, Gründungsvorstand von Digitalcourage.

Auch die Form der Speicherung ist problematisch: Für einen Abgleich der Fingerabdrücke hätte es gereicht, nur bestimmte Teilinformationen der Abdrücke zu speichern. Die EU-Vorschrift legt aber fest, dass auf den Personalausweisen Bilder des gesamten Fingerabdrucks gespeichert werden. Das widerspricht dem in der Europäischen Datenschutzgrundverordnung festgelegten Prinzip der Datenminimierung bzw. Datensparsamkeit.

Konstantin Macher von Digitalcourage meint dazu: „Erfahrungsgemäß ist bei einem Datenleck die Frage nicht ob, sondern wann es passiert. Die Speicherung unserer kompletten Fingerabdrücke vergrößert die Gefahr eines Identitätsdiebstahls, sobald der RFID-Chip geknackt ist."

Urteil des EuGH entscheidet über Speicherpflicht bei deutschen Personalausweisen

Der Fall muss nun vor dem EuGH verhandelt werden. Außer der klagenden Seite können nun zunächst auch noch die EU-Mitgliedsstaaten, die Kommission und der Generalanwalt beim EuGH Stellung nehmen. Sollte der europäische Gerichtshof die EU-Verordnung kippen, dann wäre das explizit darauf aufbauende deutsche Gesetz nicht mehr haltbar.

Mehr zum Thema auf der Website von Digitalcourage: https://digitalcourage.de/blog/2022/fingerabdruckpflicht-wird-eugh-vorgelegt

Der Vorlagebeschluss des Verwaltungsgerichts Wiesbaden als PDF: https://digitalcourage.de/sites/default/files/2022-01/Beschluss_VG_Wiesbaden_Perso_ohne_Finger.pdf

Digitalisierung und Datenschutz im Koalitionsvertrag 2021-2025 der Parteien SPD, Bündnis 90/Die Grünen, FDP:

Mehr Fortschritt wagen – Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit

(S. 4) I. Präambel - Was das Land herausfordert: … Zugleich verändert die Digitalisierung die Art und Weise wie wir wirtschaften, arbeiten und miteinander kommunizieren. …

(S. 5) Was wir voranbringen wollen: … Wir bringen eine umfassende Digitalisierung der Verwaltung voran. … Die öffentlichen Investitionen insbesondere in Klimaschutz, Digitalisierung, Bildung und Forschung werden wir im Rahmen der bestehenden Schuldenregel des Grundgesetzes gewährleisten, Anreize für private Investitionen setzen und Raum für unternehmerisches Wagnis schaffen, um so Wachstum zu generieren.

(S. 8) II. Moderner Staat, digitaler Aufbruch und Innovationen: … Ein Staat, der die Kooperation mit Wirtschaft und Zivilgesellschaft sucht, mehr Transparenz und Teilhabe in seinen Entscheidungen bietet und mit einer unkomplizierten, schnellen und digitalen Verwaltung das Leben der Menschen einfacher macht. Wir wollen das Potenzial der Digitalisierung in Staat und Gesellschaft besser nutzen. Unser Ziel ist die flächendeckende Versorgung mit Glasfaser und dem neuesten Mobilfunkstandard. Wir werden digitale Schlüsseltechnologien fördern und die Bedingungen für Start-ups am Technologiestandort verbessern. Wir haben Lust auf Neues und werden technologische, digitale, soziale und nachhaltige Innovationskraft befördern. Durch bessere Rahmenbedingungen für Hochschule, Wissenschaft und Forschung wollen wir den Wissenschaftsstandort kreativer und wettbewerbsfähiger machen.

(S. 9) Verwaltungsmodernisierung: Die Verwaltung soll agiler und digitaler werden. … Die Digitalisierung wird zu einem allgemeinen und behördenübergreifenden Kernbestandteil der Ausbildung. …

(S. 10) Transparenz: … Wir werden das Lobbyregistergesetz nachschärfen, Kontakte zu Ministerien ab Referentenebene einbeziehen und den Kreis der eintragungspflichtigen Interessenvertretungen grundrechtsschonend und differenziert erweitern. … Wir wollen die Nationalen Aktionspläne im Rahmen der Open-Government-Partnership (OGP) Deutschlands umsetzen und weiterentwickeln. … Parteiensponsoring werden wir ab einer Bagatellgrenze veröffentlichungspflichtig machen. … Wir wollen das Parteiengesetz auf den Stand der Zeit bringen und dabei insbesondere den Parteien mehr (S. 11) digitale Beschlussfassungen und im Rahmen der verfassungsrechtlichen Grenzen digitale Wahlen ermöglichen. … Die Informationsfreiheitsgesetze werden wir zu einem Bundestransparenzgesetz weiterentwickeln. …

(S. 12) Planungs- und Genehmigungsbeschleunigung: … Für eine Personal- und Weiterbildungsoffensive sowie die Digitalisierung auf allen Ebenen streben wir einen verlässlichen und nachhaltigen Pakt für Planungs-, Genehmigungs- und Umsetzungsbeschleunigung mit den Ländern an. … Die Digitalisierung von Planungs- und Genehmigungsprozessen werden wir priorisiert umsetzen. Wir werden Behörden mit notwendiger Technik ausstatten, IT-Schnittstellen zwischen Bund und Ländern standardisieren und das digitale Portal für Umweltdaten zu einem öffentlich nutzbaren zentralen Archiv für Kartierungs- und Artendaten ausbauen. Bereits erhobene Daten sind, ggf. durch Plausibilisierungen, möglichst lange nutzbar zu machen. … Die digitalen Möglichkeiten des Planungssicherstellungsgesetzes werden wir nahtlos fortsetzen und insbesondere im Hinblick auf die Bürgerbeteiligung weiterentwickeln.

(S. 15) Digitale Innovationen und digitale Infrastruktur: Deutschland braucht einen umfassenden digitalen Aufbruch. Wir wollen das Potenzial der Digitalisierung für die Entfaltungsmöglichkeiten der Menschen, für Wohlstand, Freiheit, soziale Teilhabe und Nachhaltigkeit nutzen. Dafür werden wir uns ambitionierte und überprüfbare Ziele setzen sowie realistische und schnell spürbare Maßnahmen ergreifen. Kompetenzen in der Bundesregierung werden neu geordnet und gebündelt, ein zentrales zusätzliches Digitalbudget eingeführt und Gesetze einem Digitalisierungscheck unterzogen. Die Verwaltung wird digitaler und konsequent bürgerorientiert. Wir fördern digitale Innovationen sowie unternehmerische und gesellschaftliche Initiative und setzen auf offene Standards und Diversität. Wir stärken die Digitalkompetenz, Grundrechte, Selbstbestimmung und den gesellschaftlichen Zusammenhalt. Wir sorgen für Sicherheit und Respekt auch in Zeiten des Wandels. Wir machen aus technologischem auch gesellschaftlichen Fortschritt. Dabei ist uns bewusst: Ein digitaler Aufbruch, der unsere Werte, die digitale Souveränität und einen starken Technologiestandort sichert, gelingt nur in einem fortschrittlichen europäischen Rahmen.

Digitaler Staat und digitale Verwaltung: Die Menschen erwarten vom Staat einfach handhabbare und zeitgemäße digitale Leistungen, nutzerorientiert, medienbruchfrei und flächendeckend. Lösungen durch Automation – wie die automatisierte Auszahlung der Kindergrundsicherung – setzen wir prioritär um. Die Weiterentwicklung des Onlinezugangsgesetzes (OZG) geht mit einer ausreichenden Folgefinanzierung einher, mit der eine klare Standardisierung und Vereinheitlichung von IT-Verfahren nach dem Einer-für-alle-Prinzip (EfA) unterstützt wird. Im Rahmen der IT-Konsolidierung schaffen wir

klare Verantwortlichkeiten und führen die IT-Budgets des Bundes zentral zusammen. … Digitalisierungshemmnisse (Schriftform u. a.) bauen wir mittels Generalklausel ab und vereinheitlichen Begriffe (z.B. „Einkommen"). Ein vertrauenswürdiges, allgemein anwendbares Identitätsmanagement sowie die verfassungsfeste Registermodernisierung haben Priorität. Für öffentliche IT-Projekte schreiben wir offene Standards fest. Entwicklungsaufträge werden in der Regel als Open Source beauftragt, die entsprechende Software wird grundsätzlich öffentlich gemacht. Auf Basis einer Multi-Cloud Strategie und offener Schnittstellen sowie strenger Sicherheits- und Transparenzvorgaben bauen wir eine Cloud der öffentlichen Verwaltung auf.

(S. 16) Digitale Infrastruktur: … Wir prüfen Wege hin zu einer besseren digitalen Teilhabe für alle, z.B. durch Barrierefreiheit. Wir sichern die Netzneutralität.

Bürgerrechte und IT-Sicherheit: Wir stärken digitale Bürgerrechte und IT-Sicherheit. Sie zu gewährleisten ist staatliche Pflicht. Wir führen ein Recht auf Verschlüsselung, ein wirksames Schwachstellenmanagement, mit dem Ziel Sicherheitslücken zu schließen, und die Vorgaben „security-by-design/default" ein. Auch der Staat muss verpflichtend die Möglichkeit echter verschlüsselter Kommunikation anbieten. Hersteller haften für Schäden, die fahrlässig durch IT-Sicherheitslücken in ihren Produkten verursacht werden. Die Cybersicherheitsstrategie und das IT-Sicherheitsrecht werden weiterentwickelt. Darüber hinaus sichern wir die digitale Souveränität, u. a. durch das Recht auf Interoperabilität und Portabilität sowie das Setzen auf offene Standards, Open Source und europäische Ökosysteme, etwa bei 5G oder KI. Wir leiten einen strukturellen Umbau der IT-Sicherheitsarchitektur ein, stellen das Bundesamt für Sicherheit in der Informationstechnik (BSI) unabhängiger auf und bauen es als zentrale Stelle im Bereich IT-Sicherheit aus. Wir verpflichten alle staatlichen Stellen, ihnen bekannte Sicherheitslücken beim BSI zu melden und sich regelmäßig einer externen Überprüfung ihrer IT-Systeme zu unterziehen. Das Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, z.B. in der IT-Sicherheitsforschung, soll legal durchführbar sein. Hackbacks lehnen wir als Mittel der **(S. 17)** Cyberabwehr grundsätzlich ab. Nicht-vertrauenswürdige Unternehmen werden beim Ausbau kritischer Infrastrukturen nicht beteiligt.

Nutzung von Daten und Datenrecht: Die Potenziale von Daten für alle heben wir, indem wir den Aufbau von Dateninfrastrukturen unterstützen und Instrumente wie Datentreuhänder, Datendrehscheiben und Datenspenden gemeinsam mit Wirtschaft, Wissenschaft und Zivilgesellschaft auf den Weg bringen. Wir streben einen besseren Zugang zu Daten an, insbesondere um Start-ups sowie KMU neue innovative Geschäftsmodelle und soziale Innovationen in der Digitalisierung zu ermöglichen. Ein Dateninstitut soll Datenverfügbarkeit und -standardisierung vorantreiben, Datentreuhändermodelle und Lizenzen etablieren. Für Gebietskörperschaften schaffen wir zu fairen und wettbewerbskonformen Bedingungen Zugang zu Daten von Unternehmen, insofern dies zur Erbringung ihrer Aufgaben der Daseinsvorsorge erforderlich ist. Für alle, die an der Entstehung von Daten mitgewirkt haben, stärken wir den standardisierten und maschinenlesbaren Zugang zu selbsterzeugten Daten. Mit einem Datengesetz schaffen wir für diese Maßnahmen die notwendigen rechtlichen Grundlagen. Wir fördern Anonymisierungstechniken, schaffen Rechtssicherheit durch Standards und führen die Strafbarkeit rechtswidriger De-anonymisierung ein. Wir führen einen Rechtsanspruch auf Open Data ein und verbessern die Datenexpertise öffentlicher Stellen. Die Datenschutzgrundverordnung (DSGVO) ist eine gute internationale Standardsetzung. Zur besseren Durchsetzung und Kohärenz des Datenschutzes verstärken wir die europäische Zusammenarbeit, institutionalisieren die Datenschutzkonferenz im Bundesdatenschutzgesetz (BDSG) und wollen ihr rechtlich, wo möglich, verbindliche Beschlüsse ermöglichen. Wir schaffen Regelungen zum Beschäftigtendatenschutz, um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen. Wir setzen uns für eine schnelle Verabschiedung einer ambitionierten E-Privacy-Verordnung ein.

Digitale Gesellschaft: Wir werden das digitale Ehrenamt sichtbarer machen, unterstützen und rechtlich stärken. Die Zivilgesellschaft binden wir besser in digitalpolitische Vorhaben ein und unterstützen sie, insbesondere in den Bereichen Diversität und Civic Tech. Beim Digital Services Act setzen wir uns für die Wahrung der Kommunikationsfreiheiten, starke Nutzerrechte, klare Meldeverfahren, den Zugang zu Daten sehr großer Plattformen für Forschungszwecke, die Überprüfbarkeit ihrer algorithmischen Systeme sowie klare Regelungen gegen Desinformationen ein. Auf Grundlage der europäischen Vorgaben werden wir den Rechtsrahmen (u. a. Telemediengesetz, TMG und Netzwerkdurchsetzungsgesetz, NetzDG) grundlegend überarbeiten. Den Aufbau von Plattformräten werden wir voranbringen. Allgemeine Überwachungspflichten, Maßnahmen zum Scannen privater Kommunikation und eine **(S. 18)** Identifizierungspflicht lehnen wir ab. Anonyme und pseudonyme Online-Nutzung werden wir wahren. Mit einem Gesetz gegen digitale Gewalt werden wir rechtliche Hürden für Betroffene, wie Lücken bei Auskunftsrechten, abbauen und umfassende Beratungsangebote aufsetzen. Wir schaffen die rechtlichen Rahmenbedingungen für elektronische Verfahren zur Anzeigenerstattung und für private Verfahren und ermöglichen richterlich angeordnete Accountsperren. Wir werden die Einrichtung einer Bundeszentrale für digitale Bildung prüfen.

Digitale Schlüsseltechnologien: … Investitionen in Künstliche Intelligenz (KI), Quantentechnologien, Cybersicherheit, Distributed-Ledger-Technologie (DLT), Robotik und weitere Zukunftstechnologien stärken wir messbar und setzen Schwerpunkte. Wir stärken strategische Technologiefelder z.B. durch Important Projects of Common European Interest (IPCEIs) und treiben den angekündigten EU Chips Act voran. Mit europäischen Partnerländern fördern wir die Zusammenarbeit starker europäischer Forschungsstandorte, insbesondere bei KI, und ermöglichen institutionelle Freiräume. Im Sinne eines lernenden, technologiefördernden Staates setzen wir digitale Innovationen in der Verwaltung ein, schaffen notwen-

dige Rechtsgrundlagen und Transparenz. Wir unterstützen den europäischen AI Act. Wir setzen auf einen mehrstufigen risikobasierten Ansatz, wahren digitale Bürgerrechte, insbesondere die Diskriminierungsfreiheit, definieren Haftungsregeln und vermeiden innovationshemmende ex-ante-Regulierung. Biometrische Erkennung im öffentlichen Raum sowie automatisierte staatliche Scoring Systeme durch KI sind europarechtlich auszuschließen. …

(S. 19) Digitale Wirtschaft: Wir unterstützen ein Level Playing Field im Wettbewerb und setzen uns für ambitionierte Regelungen des Digital Markets Act (DMA) ein, die nicht hinter bestehende nationale Regeln zurückfallen dürfen. Dazu gehören auch europäisch einheitliche Interoperabilitätsverpflichtungen und Regelungen zur Fusionskontrolle. Das Bundeskartellamt stärken wir im Umgang mit Plattformen. Wir fördern digitale Startups in der Spätphasenfinanzierung und stärken den Venture-Capital-Standort. Wir wollen den Anteil von Gründerinnen im Digitalsektor erhöhen. Dafür schaffen wir ein Gründerinnen-Stipendium und reservieren einen Teil des Zukunftsfonds. Öffentliche Ausschreibungen und Beschaffungsprozesse gestalten wir z.B. für Gov- und EduTech-Start-ups einfacher. Wir werden die Mitarbeiterkapitalbeteiligung für Start-ups attraktiver gestalten. Wir stärken den Games-Standort Deutschland und verstetigen die Förderung. Wir stärken KMU bei der Digitalisierung durch unkomplizierte Förderung und bauen die Unterstützung für IT-Sicherheit, DSGVO-konforme Datenverarbeitung und den Einsatz digitaler Technologien aus.

(S. 20) Zukunftsstrategie Forschung: … Zentrale Zukunftsfelder sind unter anderem: … Drittens: ein vorsorgendes, krisenfestes und modernes Gesundheitssystem, welches die Chancen biotechnologischer und medizinischer Verfahren nutzt, und das altersabhängige Erkrankungen sowie seltene oder armutsbedingte Krankheiten bekämpft. Viertens: technologische Souveränität und die Potentiale der Digitalisierung, z.B. in Künstlicher Intelligenz und Quantentechnologie, für datenbasierte Lösungen quer durch alle Sektoren. …

(S. 21) Forschungsdaten: Das ungenutzte Potential, das in zahlreichen Forschungsdaten liegt, wollen wir effektiver für innovative Ideen nutzen. Den Zugang zu Forschungsdaten für öffentliche und private Forschung wollen wir mit einem Forschungsdatengesetz umfassend verbessern sowie vereinfachen und führen Forschungsklauseln ein. Open Access wollen wir als gemeinsamen Standard etablieren. Wir setzen uns für ein wissenschaftsfreundlicheres Urheberrecht ein. Die Nationale Forschungsdateninfrastruktur wollen wir weiterentwickeln und einen Europäischen Forschungsdatenraum vorantreiben. Datenteilung von vollständig anonymisierten und nicht personenbezogenen Daten für Forschung im öffentlichen Interesse wollen wir ermöglichen.

(S. 24) Wissenschaftskommunikation und Partizipation: … Wir setzen uns für die Förderung des Wissenschaftsjournalismus durch eine unabhängige Stiftung, Weiterbildung für Entscheidungsträgerinnen und Entscheidungsträger, analoge und digitale Orte – von Forschungsmuseen bis Dashboards – ein. Wir werden mit Citizen Science und Bürgerwissenschaften Perspektiven aus der Zivilgesellschaft stärker in die Forschung einbeziehen. Open Access und Open Science wollen wir stärken.

(S. 25) Industrie: Der Industrie kommt eine zentrale Rolle bei der Transformation der Wirtschaft mit Blick auf Klimaschutz und Digitalisierung zu. …

(S. 29) Gesundheitswirtschaft: Eine innovative Gesundheitswirtschaft ist Grundlage des weiteren medizinischen Fortschritts und birgt gleichzeitig viel Potenzial für Beschäftigung und Wohlstand. Wir wollen weiter in Forschung investieren, um medizinische Spitzenleistungen (wie u. a. aktuell die Anwendung der mRNA-Impfstoffe) zu ermöglichen. Wir setzen uns für High-Medizintechnik „made in Germany" ein. Zugleich wollen wir die Potenziale der Digitalisierung nutzen, um eine bessere Versorgungsqualität zu erreichen, aber auch Effizienzpotenziale zu heben. Damit die Beschäftigten des Gesundheitswesens die digitale Transformation bewältigen können, sind frühzeitige Weiterbildungsangebote unerlässlich. …

(S. 31) Fairer Wettbewerb: … Wir wollen eine Verpflichtung zur Interoperabilität auf europäischer Ebene und über das GWB für marktbeherrschende Unternehmen verankern. Dabei sollen – basierend auf internationalen technischen Standards – das Kommunikationsgeheimnis, ein hoher Datenschutz und hohe IT-Sicherheit sowie eine durchgängige Ende-zu-Ende-Verschlüsselung sichergestellt werden. Die Datenportabilität soll gestärkt werden. Auf EU-Ebene setzen wir uns außerdem für eine Verabschiedung eines ambitionierten Digital Markets Act (DMA) sowie seine Durchsetzung durch die Wettbewerbsbehörden der Mitgliedstaaten ein. Auf europäischer Ebene werden wir uns für eine Anpassung der Fusionskontrolle zur Unterbindung innovationshemmender strategischer Aufkäufe potenzieller Wettbewerber (sogenannte killer-acquisitions) einsetzen.

(S. 32) Bürokratieabbau: … Wir werden das „Once-only"-Prinzip schnellstmöglich einführen. Das bereits beschlossene Unternehmens-Basisdatenregister soll schnell umgesetzt und dessen Finanzierung gesichert werden. Wir werden prüfen, inwiefern wir den Aufwand für und durch die rein elektronische Aufbewahrung von Belegen und Geschäftsunterlagen verringern können. …

(S. 34) Vergaberecht: … Wir wollen die rechtssichere Digitalisierung in diesem Bereich vorantreiben und dazu eine anwenderfreundliche zentrale Plattform schaffen, über die alle öffentlichen Vergaben zugänglich sind und die eine Präqualifizierung der Unternehmen ermöglicht. Wir wollen schnelle Entscheidungen bei Vergabeverfahren der öffentlichen Hand fördern und unterstützen dabei Länder und Kommunen bei der Vereinfachung, Digitalisierung und Nachhaltigkeit. …

(S. 47) Digitalisierung in der Landwirtschaft: Wir werden die von der Landwirtschaft und Ernährung benötigten öffentlichen Daten einfacher und in geeigneter Qualität und Aktualität den berechtigten Nutzern frei zur Verfügung stellen und dazu eine echte Plattform mit zentralem Zugang zu sämtlichen staatlichen Daten und Diensten einrichten, insbesondere auch für entsprechende Verwaltungsdienstleistungen. Staatliche Daten aller Verwaltungsebenen sollen künftig in einheitlichen Formaten zur Verfügung gestellt werden. Der Agrardatenraum in Gaia-X als Basis einer europäischen Dateninfrastruktur

mit klarem Nutzungsrecht für Landwirte an den betriebsspezifischen Daten, an deren Entstehung sie mitgewirkt haben, wird mit standardisierten Schnittstellen weiterentwickelt. Open-Source-Formate werden ausdrücklich unterstützt. …

(S. 50) Öffentlicher Verkehr und neue Mobilitätsangebote: … Für eine nahtlose Mobilität verpflichten wir Verkehrsunternehmen und Mobilitätsanbieter, ihre Echtzeitdaten unter fairen Bedingungen bereitzustellen. Anbieterübergreifende digitale Buchung und Bezahlung wollen wir ermöglichen. Den Datenraum Mobilität entwickeln wir weiter. …

(S. 52) Autoverkehr: … Wir schaffen ein Mobilitätsdatengesetz und stellen freie Zugänglichkeit von Verkehrsdaten sicher. Zur wettbewerbsneutralen Nutzung von Fahrzeugdaten streben wir ein Treuhänder-Modell an, das Zugriffsbedürfnisse der Nutzer, privater Anbieter und staatlicher Organe sowie die Interessen betroffener Unternehmen und Entwickler angemessen berücksichtigt. Im Gesetz zum autonomen Fahren werden wir die Regelungen verbessern, Haftungsfragen klären und die Datenhoheit der Nutzer sicherstellen. …

Verkehrsordnung: … Wir wollen eine Öffnung für digitale Anwendungen wie digitale Parkraumkontrolle. …

(S. 71) Mitbestimmung: … Die sozialökologische Transformation und die Digitalisierung kann nur mit den Arbeitnehmerinnen und Arbeitnehmern wirksam gestaltet werden. Hinsichtlich dieser Fragen werden wir das Betriebsrätemodernisierungsgesetz evaluieren. …

(S. 72) Digitale Plattformen: Digitale Plattformen sind eine Bereicherung für die Arbeitswelt, deswegen sind gute und faire Arbeitsbedingungen wichtig. In diesem Sinne überprüfen wir bestehendes Recht und verbessern die Datengrundgrundlagen. Dazu führen wir den Dialog mit Plattformanbietern, -arbeitern, Selbständigen sowie Sozialpartnern. Die Initiative der EU-Kommission zur Verbesserung der Arbeitsbedingungen auf Plattformen begleiten wir konstruktiv. Bei der Gestaltung von KI in der Arbeitswelt setzen wir auf einen menschenzentrierten Ansatz, soziale und wirtschaftliche Innovation ebenso wie Gemeinwohlorientierung. Wir unterstützen den risikobasierten EU-Ansatz. …

(S. 82) Pflege: … Wir bringen ein allgemeines Heilberufegesetz auf den Weg und entwickeln das elektronische Gesundheitsberuferegister weiter.

(S. 83) Digitalisierung im Gesundheitswesen: In einer regelmäßig fortgeschriebenen Digitalisierungsstrategie im Gesundheitswesen und in der Pflege legen wir einen besonderen Fokus auf die Lösung von Versorgungsproblemen und die Perspektive der Nutzerinnen und Nutzer. In der Pflege werden wir die Digitalisierung u. a. zur Entlastung bei der Dokumentation, zur Förderung sozialer Teilhabe und für therapeutische Anwendungen nutzen. Wir ermöglichen regelhaft telemedizinische Leistungen inklusive Arznei-, Heil- und Hilfsmittelverordnungen sowie Videosprechstunden, Telekonsile, Telemonitoring und die telenotärztliche Versorgung. Wir beschleunigen die Einführung der elektronischen Patientenakte (ePA) und des E-Rezeptes sowie deren nutzenbringende Anwendung und binden beschleunigt sämtliche Akteure an die Telematikinfrastruktur an. Alle Versicherten bekommen DSGVO-konform eine ePA zur Verfügung gestellt; ihre Nutzung ist freiwillig (opt-out). Die gematik bauen wir zu einer digitalen Gesundheitsagentur aus. Zudem bringen wir ein Registergesetz und ein Gesundheitsdatennutzungsgesetz zur besseren wissenschaftlichen Nutzung in Einklang mit der DSGVO auf den Weg und bauen eine dezentrale Forschungsdateninfrastruktur auf.

(S. 84) Wir überprüfen das SGB V und weitere Normen hinsichtlich durch technischen Fortschritt überholter Dokumentationspflichten. Durch ein Bürokratieabbaupaket bauen wir Hürden für eine gute Versorgung der Patientinnen und Patienten ab. Die Belastungen durch Bürokratie und Berichtspflichten jenseits gesetzlicher Regelungen werden kenntlich gemacht. Wir verstetigen die Verfahrenserleichterungen, die sich in der Pandemie bewährt haben. Sprachmittlung auch mit Hilfe digitaler Anwendungen wird im Kontext notwendiger medizinischer Behandlung Bestandteil des SGB V. …

(S. 86) Rechte von Patientinnen und Patienten: Die Unabhängige Patientenberatung (UPD) überführen wir in eine dauerhafte, staatsferne und unabhängige Struktur unter Beteiligung der maßgeblichen Patientenorganisationen. …

(S. 89) Bauen und Wohnen, Digitalisierung und Vereinfachung: Wir werden durch serielles Bauen, Digitalisierung, Entbürokratisierung und Standardisierung die Kosten für den Wohnungsbau senken. … Wir werden die Bau- und Immobilienwirtschaft sowie alle Ebenen der Verwaltung unterstützen die Digitalisierung zu meistern, Open-BIM und einheitliche Schnittstellen/Standards umzusetzen. Der Bundesbau ist Vorbild bei der Digitalisierung und unseren bau-, wohnungs- und klimapolitischen Zielen.

… Wir werden die entsprechenden Regelungen im Baulandmobilisierungsgesetz entfristen und die rechtlichen Grundlagen für eine vollständige Digitalisierung der Bauleitplanverfahren schaffen. …

(S. 91) Schutz der Mieterinnen und Mieter: … Wir werden qualifizierte Mietspiegel stärken, verbreitern und rechtssicher ausgestalten. Zur Berechnung sollen die Mietverträge der letzten sieben Jahre herangezogen werden. Wir werden für mehr Transparenz bei den Nebenkostenabrechnungen sorgen. …

(S. 92) Städtebau: … Wir entwickeln den Smart-City-Stufenplan weiter, stärken BIM Deutschland und richten ein Smart-City-Kompetenzzentrum ein. …

(S. 93) V. Chancen für Kinder, starke Familien und beste Bildung ein Leben lang: Wir wollen allen Menschen unabhängig von ihrer Herkunft beste Bildungschancen bieten, Teilhabe und Aufstieg ermöglichen und durch inklusive Bildung sichern. Dazu stärken wir die frühkindliche Bildung, legen den Digitalpakt 2.0 auf und machen das BAföG elternunabhängiger und bauen es für die Förderung der beruflichen Weiterbildung aus. …

(S. 96) Digitalpakt Schule: Wir wollen Länder und Kommunen dauerhaft bei der Digitalisierung des Bildungswesens unterstützen. Den Mittelabruf beim Digitalpakt Schule werden wir beschleunigen und entbürokratisieren. … Dieser Digitalpakt wird auch die nachhaltige Neuanschaffung von Hardware, den Austausch veralteter Technik sowie die Gerätewartung und Administration umfassen. … Wir werden gemeinsam mit den Ländern digitale Programmstruktu-

ren und Plattformen für Open Educational Ressources (OER), die Entwicklung intelligenter, auch lizenzfreier Lehr- und Lernsoftware sowie die Erstellung von Positivlisten datenschutzkonformer, digitaler Lehr- und Lernmittel unterstützen.

(S. 99) Kinder und Jugend: … Wir werden Angebote der Jugendhilfe bei der Digitalisierung unterstützen. …

(S. 102) Familienrecht: … Das Samenspenderregister wollen wir auch für bisherige Fälle, private Samenspenden und Embryonenspenden öffnen. …

(S. 103) VI. Freiheit und Sicherheit, Gleichstellung und Vielfalt in der modernen Demokratie: Freiheit, Sicherheit und Rechtsstaatlichkeit sind die Grundlagen für das friedliche Zusammenleben in Deutschland. Wir stellen uns allen verfassungsfeindlichen, gewaltbereiten Bestrebungen und Verschwörungsideologien entschieden entgegen. Leben in Freiheit braucht Sicherheit. Unsere Verantwortung ist die Sicherheit der Bürgerinnen und Bürger. Dafür die Sicherheitsbehörden, den Bevölkerungsschutz und die Justiz. Sicherheitsgesetze und deren Auswirkungen auf Bürgerrechte werden wir im Lichte der technischen Entwicklung einer unabhängigen wissenschaftlichen Evaluation unterziehen. …

(S. 104) Bundespolizeien: … Die in anderen Bereichen bewährte Sicherheitsüberprüfung von Bewerberinnen und Bewerbern weiten wir aus und stärken so die Resilienz der Sicherheitsbehörden gegen demokratiefeindliche Einflüsse. … Wir führen eine unabhängige Polizeibeauftragte bzw. einen unabhängigen Polizeibeauftragten für die Polizeien des Bundes als Anlaufstelle beim Deutschen Bundestag mit Akteneinsichts- und Zutrittsrechten ein. Wir führen die pseudonyme Kennzeichnung von Polizistinnen und Polizisten ein.

Sichere und leistungsfähige Datenverarbeitung, kombiniert mit mobiler IT und klar geregelten Kompetenzen, sind Grundvoraussetzung moderner Polizeiarbeit. Wir entwickeln die Strategie Polizei 20/20 weiter. Wir unterziehen die umfangreiche Anzahl von Datenbanken einer grundlegenden Revision und präzisieren deren Verarbeitungsregelungen. Den Rechtsschutz sowie die Datenaufsicht durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) stärken wir deutlich. Wir öffnen die Polizei stärker für unabhängige Forschung. …

(S. 105) Zusammenarbeit von Polizei und Justiz: Wir intensivieren die grenzüberschreitende polizeiliche und justizielle Zusammenarbeit rechtsstaatlich, sichern dabei hohe Datenschutzstandards und verbessern den grenzüberschreitenden Rechtsschutz. Wir streben die Weiterentwicklung von Europol zu einem Europäischen Kriminalamt mit eigenen operativen Möglichkeiten an. … Wir wollen mit den Ländern die Aussagekraft der Kriminal- und Strafrechtspflegestatistiken nachhaltig verbessern. Wir verankern den periodischen Sicherheitsbericht gesetzlich. Wir verstetigen mit den Ländern den Pakt für den Rechtsstaat und erweitern ihn um einen Digitalpakt für die Justiz. …

(S. 106) Justiz: … Wir bauen den kollektiven Rechtsschutz aus. Bestehende Instrumente wie z.B. nach dem Kapitalanleger-Musterverfahrensgesetz modernisieren wir und prüfen den Bedarf für weitere. Die EU-Verbandsklagerichtlinie setzen wir anwenderfreundlich und in Fortentwicklung der Musterfeststellungsklage um und eröffnen auch kleinen Unternehmen diese Klagemöglichkeiten. An den bewährten Anforderungen an klageberechtigte Verbände halten wir fest. … Gerichtsentscheidungen sollen grundsätzlich in anonymisierter Form in einer Datenbank öffentlich und maschinenlesbar verfügbar sein. …

(S. 107) Kampf gegen Extremismus: … Datenbanken in der EU wollen wir kompatibel ausgestalten, die Gefährder-Definitionen vereinheitlichen, deren Früherkennung forcieren und für eine koordinierte Überwachung sorgen. Wir verbessern die Erfassung der politisch motivierten Kriminalität, z.B. in Hinblick auf frauen- und queerfeindliche Hasskriminalität. … Wir verbessern die Möglichkeit von Auskunftssperren im Melderegister für Bedrohte. …

(S. 108) Kampf gegen Kindesmissbrauch: Im Kampf gegen Kindesmissbrauch stärken wir das Bundeskriminalamt (BKA) personell und entlasten die Beschäftigten bei der Auswertung der beschlagnahmten Datenträger durch technische Lösungen – unter Sicherstellung des Schutzes personenbezogener Daten der Opfer – und realisieren den tagesaktuellen Abgleich mit den Datenbanken. Die Informationsweitergabe zwischen den Ämtern und den am Hilfenetzwerk des Kindes beteiligten Akteurinnen und Akteuren muss verbessert und verbindlicher geregelt werden – unter Wahrung des Datenschutzes und Achtung der Vertrauensstellung der Jugendämter. …

Waffenrecht, Sicherheitsdienste: … Wir evaluieren die Waffenrechtsänderungen der vergangenen Jahre und gestalten bestehende Kontrollmöglichkeiten gemeinsam mit den Schützen- und Jagdverbänden sowie mit den Ländern effektiver aus. Zudem verbessern wir die kriminalstatistische Erfassung von Straftaten mit Schusswaffen sowie den Informationsfluss zwischen den Behörden. … Private Sicherheitsdienste werden wir mit verbindlichen Standards in einem eigenen Gesetz regulieren.

Freiheit und Sicherheit: … Die Eingriffe des Staates in die bürgerlichen Freiheitsrechte müssen stets gut begründet und in ihrer Gesamtwirkung betrachtet werden. Die Sicherheitsgesetze wollen wir auf ihre tatsächlichen und rechtlichen Auswirkungen sowie auf ihre Effektivität hin evaluieren. Deshalb erstellen wir eine Überwachungsgesamtrechnung und bis spätestens Ende 2023 eine unabhängige wissenschaftliche Evaluation der Sicherheitsgesetze und ihrer Auswirkungen auf Freiheit und Demokratie im Lichte **(S. 109)** technischer Entwicklungen. Jede zukünftige Gesetzgebung muss diesen Grundsätzen genügen. Dafür schaffen wir ein unabhängiges Expertengremium (Freiheitskommission), das bei zukünftigen Sicherheitsgesetzgebungsvorhaben berät und Freiheitseinschränkungen evaluiert.

Videoüberwachung kann die Präsenz einer bürgernahen Polizei nicht ersetzen, sie aber an Kriminalitätsschwerpunkten ergänzen. Flächendeckende Videoüberwachung und den Einsatz von biometrischer Erfassung zu Überwachungszwecken lehnen wir ab. Das Recht auf Anonymität sowohl im öffentlichen Raum als auch im Internet ist zu gewährleisten.

Angesichts der gegenwärtigen rechtlichen Unsicherheit, des bevorstehenden Urteils des Europäischen Gerichts-

hofs und der daraus resultierenden sicherheitspolitischen Herausforderungen werden wir die Regelungen zur Vorratsdatenspeicherung so ausgestalten, dass Daten rechtssicher anlassbezogen und durch richterlichen Beschluss gespeichert werden können.

Mit der Login-Falle wollen wir grundrechtsschonende und freiheitsorientierte Instrumente schaffen, um die Identifizierung der Täterinnen und Täter zu erreichen.

Die Ausnutzung von Schwachstellen von IT-Systemen steht in einem hochproblematischen Spannungsverhältnis zur IT-Sicherheit und den Bürgerrechten. Der Staat wird daher keine Sicherheitslücken ankaufen oder offenhalten, sondern sich in einem Schwachstellenmanagement unter Federführung eines unabhängigeren Bundesamtes für Sicherheit in der Informationstechnik immer um die schnellstmögliche Schließung bemühen.

Für den Einsatz von Überwachungssoftware, auch kommerzieller, setzen wir die Eingriffsschwellen hoch und passen das geltende Recht so an, dass der Einsatz nur nach den Vorgaben des Bundesverfassungsgerichtes für die Online-Durchsuchung zulässig ist. Die Befugnis des Verfassungsschutzes zum Einsatz von Überwachungssoftware wird im Rahmen der Überwachungsgesamtrechnung überprüft. Das Bundespolizeigesetz novellieren wir ohne die Befugnis zur Quellen-TKÜ und Online-Durchsuchung. Solange der Schutz des Kernbereichs privater Lebensgestaltung nicht sichergestellt ist, muss ihr Einsatz unterbleiben. Transparenz und effektive Kontrolle durch Aufsichtsbehörden und Parlament werden wir sicherstellen.

Wir schaffen für die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZiTis) und in enger Abstimmung mit den Ländern für die gemeinsamen Zentren (GTAZ etc.) gesetzliche Grundlagen, legen **(S. 110)** die Verantwortlichkeiten klarer fest und garantieren die lückenlose Kontrolle durch Parlamente und Datenschutzaufsichtsbehörden. Zum Schutz der Informations- und Meinungsfreiheit lehnen wir verpflichtende Uploadfilter ab.

Nachrichtendienste sind ein wichtiger Teil der wehrhaften Demokratie. Wir achten das verfassungsrechtliche Trennungsgebot von Polizei und Nachrichtendiensten. Wir stärken und bauen die Kontrolle, insbesondere die parlamentarische, aller nachrichtendienstlichen Tätigkeiten des Bundes weiter aus. Das Sicherheitsrecht des Bundes, einschließlich der Übermittlungsvorschriften reformieren wir umfassend. Hilfsorgane der Parlamentarischen Kontrolle stärken wir. Die Wahrnehmung der Rechte Betroffener verbessern wir. Kontrolllücken schließen wir. Die Arbeit der Dienste wird durch eine fundierte wissenschaftliche Analyse gestärkt und differenziert. Wir schaffen eine unabhängige Kontrollinstanz für Streitfragen bei VS-Einstufungen und verkürzen die archivrechtlichen Schutzfristen auf maximal 30 Jahre.

Wir regeln Voraussetzungen für den Einsatz von V-Personen, Gewährspersonen und sonstigen Informantinnen und Informanten aller Sicherheitsbehörden gesetzlich und machen sie unter Wahrung der notwendigen Anonymität parlamentarisch überprüfbar. Wir prüfen, ob die Nachrichtendienste bei der Nachverfolgung von Transaktionen zur Terrorismusfinanzierung über ausreichende Möglichkeiten verfügen. …

(S. 111) Unternehmensrecht: … Wir setzen die EU-Whistleblower-Richtlinie rechtssicher und praktikabel um. Whistleblowerinnen und Whistleblower müssen nicht nur bei der Meldung von Verstößen gegen EU-Recht vor rechtlichen Nachteilen geschützt sein, sondern auch von erheblichen Verstößen gegen Vorschriften oder sonstigem erheblichen Fehlverhalten, dessen Aufdeckung im besonderen öffentlichen Interesse liegt. … Wir erleichtern die Gründung von Gesellschaften, indem wir die Digitalisierung des Gesellschaftsrechts vorantreiben und Beurkundungen per Videokommunikation auch bei Gründungen mit Sacheinlage **(S. 112)** und weiteren Beschlüssen erlauben. Wir ermöglichen dauerhaft Online-Hauptversammlungen und wahren dabei die Aktionärsrechte uneingeschränkt. Wir untersuchen weitere Vorkehrungen gegen den Missbrauch von Kostenerstattungen für Abmahnungen nach dem Gesetz gegen Unlauteren Wettbewerb (UWG). Wir erweitern den Rechtsrahmen für Legal Tech-Unternehmen, legen für sie klare Qualitäts- und Transparenzanforderungen fest und stärken die Rechtsanwaltschaft, indem wir das Verbot von Erfolgshonoraren modifizieren und das Fremdbesitzverbot prüfen.

Schutz der Verbraucherinnen und Verbraucher: Wir gewährleisten hohe Verbraucherschutzstandards. Dazu gehören eine umfassende Verbraucherbildung, mehrsprachige Aufklärung und der situationsgerechte Zugang zu Informationen. …

(S. 114) Gleichstellung: … Wir werden den Gender Data Gap schließen, z.B. im medizinischen Bereich. …

Schutz vor Gewalt: … Die Istanbul-Konvention setzen wir auch im digitalen Raum und mit einer staatlichen Koordinierungsstelle vorbehaltlos und **(S. 115)** wirksam um. …

Ökonomische Gleichstellung: … Wir wollen die Lohnlücke zwischen Frauen und Männern schließen. Deshalb werden wir das Entgelttransparenzgesetz weiterentwickeln und die Durchsetzung stärken, indem wir Arbeitnehmerinnen und Arbeitnehmern ermöglichen, ihre individuellen Rechte durch Verbände im Wege der Prozessstandschaft geltend machen zu lassen. …

(S. 120) Rassismus bekämpfen: … Wir stärken die Arbeit gegen Hass im Netz und Verschwörungsideologien. …

(S. 121) Antidiskriminierung: … Das Allgemeine Gleichbehandlungsgesetz (AGG) werden wir evaluieren, Schutzlücken schließen, den Rechtsschutz verbessern und den Anwendungsbereich ausweiten. …

(S. 122) Kulturförderung: … Wir fördern den Aufbau eines Datenraums Kultur, der sparten- und länderübergreifend Zugang zu Kultur ermöglicht. …

(S. 123) … Wir wollen den Games-Standort stärken und die Förderung verstetigen. …

Rechtliche Rahmenbedingungen: Beim Urheberrecht setzen wir uns für fairen Interessenausgleich ein und wollen die Vergütungssituation für kreative und journalistische Inhalte verbessern, auch in digitalen Märkten. …

(S. 124) Medien: … Auf europäischer Ebene setzen wir uns dafür ein, dass Digital Service Act (DSA) und Digital Markets Act (DMA) sowie Media Freedom Act auch Pluralismus und Vielfalt abbilden sowie eine staatsferne Medien-

aufsicht und Regulierung gewährleisten. Wir werden die Machbarkeit einer technologieoffenen, barrierefreien und europaweiten Medienplattform prüfen. … Die Herausforderungen der digitalen Transformation der Medienlandschaft wollen wir durch faire Regulierung der Plattformen und Intermediäre begleiten, um kommunikative Chancengleichheit sicherzustellen. Wir schaffen eine gesetzliche Grundlage für den Auskunftsanspruch der Presse gegenüber Bundesbehörden. Wir bekämpfen Hassrede und Desinformation. …

Wir werden die Bundesstiftung Aufarbeitung stärken. Wir werden die festgeschriebenen Standorte der Außenstellen des Stasi-Unterlagen-Archivs qualitativ entwickeln. Die begleitende Forschungs- und Bildungsarbeit wird unterstützt. Wir unterstützen die Einrichtung des Archivzentrums SED-Diktatur und die Weiterentwicklung der ehemaligen Stasi-Zentrale in Berlin zum Campus für Demokratie. …

(S. 128) Gute Lebensverhältnisse in Stadt und Land: … Alle Bundesförderprogramme werden regelmäßig evaluiert und auf ihre räumliche Wirkung mit einheitlichen Datenstandards überprüft. … Wir wollen die Chancen der Digitalisierung für Stadt und Land besser erschließen. Der Bund schafft die Voraussetzungen, dass das OZG in den Kommunen erfolgreich und praktikabel umgesetzt werden kann. Das Bundesprogramm Smart Cities wird fortgeschrieben und erweitert auf Smart Regions, dabei soll es agiler gestaltet und mit städtebaulichen Fragen verknüpft werden. …

(S. 132) Zukunft der Europäischen Union: … Die strategische Souveränität Europas wollen wir erhöhen. Dies bedeutet in erster Linie eigene Handlungsfähigkeit im globalen Kontext herzustellen und in wichtigen strategischen Bereichen, wie Energieversorgung, Gesundheit, Rohstoffimporte und digitale Technologie, weniger abhängig und verwundbar zu sein, ohne Europa abzuschotten. …

(S. 134) Krisenfestes Europa: … Um die EU-Gesundheitsbehörden krisenfest zu machen, statten wir diese mit den erforderlichen Kompetenzen und Ressourcen aus. Die Potenziale des Europäischen Gesundheitsdatenraumes sollen bei Wahrung **(S. 135)** von Datenschutz und Patientensouveränität erschlossen und der Kampf gegen Antibiotikaresistenz verstärkt werden.

(S. 137) Europäische Freizügigkeit: … Wir brauchen einen Digitalisierungsschub zum Abbau von Bürokratie, zur einfachen Handhabung von Freizügigkeit, schnelleren Geltendmachung bestehender Ansprüche sowie zur Erleichterung des Kampfs gegen Betrug und Missbrauch. Daher unterstützen wir einen neuen Anlauf zur Einführung einer Europäischen Sozialversicherungsnummer, auch um die Geltendmachung bestehender Portabilitätsansprüche zu erleichtern. …

(S. 138) Aufenthalts- und Bleiberecht: … Wir werden die Klärung der Identität einer Ausländerin oder eines Ausländers um die Möglichkeit, eine Versicherung an Eides statt abzugeben, erweitern und werden hierzu eine gesetzliche Regelung im Ausländerrecht schaffen. …

(S. 142) Europäische und internationale Flüchtlingspolitik: … Wir werden humanitäre Visa für gefährdete Personen ermöglichen und dazu digitale Vergabeverfahren einführen. …

(S. 143) … Die strategische Souveränität Europas wollen wir erhöhen. Ziel ist eine multilaterale Kooperation in der Welt, insbesondere in enger Verbindung mit denjenigen Staaten, die unsere demokratischen Werte teilen. Dabei geht es auch um den Systemwettbewerb mit autoritär regierten Staaten und eine strategische Solidarität mit unseren demokratischen Partnern. Die Menschenrechte als wichtigster Schutzschild der Würde des Einzelnen bilden dabei unseren Kompass.

(S. 144) Multilateralismus: … Deutschland betreibt eine aktive digitale Außenpolitik für ein globales, offenes Internet und eine konsistente EU-Digitalpolitik über Ressortgrenzen hinweg. Wir stärken unseren Einsatz in internationalen Gremien, Normen- und Standardisierungsprozessen sowie Multi-Stakeholder-Foren (z.B. IGF). Den Einsatz der globalen Zivilgesellschaft für digitale Bürgerrechte unterstützen wir. Wir wollen ein Völkerrecht des Netzes. In der Entwicklungszusammenarbeit arbeiten wir mit unseren Partnern am Aufbau ihrer unabhängigen digitalen Infrastruktur zur Stärkung ihrer digitalen Souveränität, auch auf EU-Ebene. Wir verfolgen im digitalen Raum eine Politik der Abrüstung. Dazu gehören auch ein Stopp der Weitergabe von Überwachungstechnologien an repressive Regime sowie der Schutz ziviler Infrastruktur vor Cyberangriffen.

(S. 147) Menschenrechte: … Wir wollen den Schutz der Menschenrechte im digitalen Zeitalter stärken und hierfür die Internetfreiheit und digitale Menschenrechte zu außenpolitischen Schwerpunkten machen. Die Initiative zum Recht auf Privatheit unterstützen wir. …

(S. 149) Verteidigung und Bundeswehr: … Den neuen Bedrohungen im Cyberspace wollen wir durch eine ehrgeizige Cybersicherheitspolitik entgegentreten. Die Bundeswehr muss zudem in die Lage versetzt werden, im Verbund mit anderen Bundesbehörden im Cyber- und Informationsraum als Akteur erfolgreich zu bestehen. Die parlamentarische Kontrolle über den Einsatz von Cyber-Fähigkeiten der Bundeswehr muss gewährleistet sein. …

(S. 150) Alle Angehörigen der Bundeswehr müssen unzweifelhaft auf dem Boden der freiheitlich demokratischen Grundordnung stehen. …

(S. 158) VIII. Zukunftsinvestitionen und nachhaltige Finanzen: Die 2020er Jahre wollen wir zu einem Jahrzehnt der Zukunftsinvestitionen, insbesondere in Klimaschutz, Digitalisierung, Bildung und Forschung sowie die Infrastruktur, machen. Wir verfolgen dazu eine Politik, die die Investitionen – privat, wie öffentlich – deutlich erhöht. …

(S. 159) Zukunftsinvestitionen: Wir wollen mehr privates Kapital für Transformationsprojekte aktivieren. … Um eine Erhöhung des Finanzierungsvolumens insbesondere für die Klima- und Digitalisierungstransformation der Wirtschaft und von Privathaushalten zu erreichen, werden wir das bewährte Förderinstrumentarium bedarfsgerecht und nach Maßgabe der Zielgenauigkeit und Fördereffizienz skalieren und ausweiten. …

(S. 166) Vollzug, Vereinfachung und Digitalisierung: Das strategische Vorgehen gegen Steuerhinterziehung, Finanzmarktkriminalität und Geldwäsche werden wir im Bundesfinanzministerium organisatorisch und personell stärken, und dabei auch Zoll, Bundes-

zentralamt für Steuern (BZSt), Bundesanstalt für Finanzdienstleistungen (BaFin) und die Financial Intelligence Unit (FIU) stärken. Durch digitale Verfahren soll die Erfüllung der steuerlichen Pflichten für die Bürgerinnen und Bürger erleichtert werden, wie zum Beispiel durch vorausgefüllte Steuererklärungen (Easy Tax). Wir werden daher die Digitalisierung des Besteuerungsverfahrens konsequent weiter vorantreiben und dafür sorgen, dass steuerliche Regelungen grundsätzlich auch digital umsetzbar sind. Unser Ziel ist es, das die gesamte Interaktion zwischen Steuerpflichtigen und Finanzverwaltung digital möglich ist.

Im Bereich der Unternehmensbesteuerung ist es uns ein Anliegen, die Steuerprüfung zu modernisieren und zu beschleunigen. Dafür setzen wir uns insbesondere für verbesserte Schnittstellen, Standardisierung und den sinnvollen Einsatz neuer Technologien ein. Zur Sicherung der Anschlussfähigkeit der Steuerverwaltung an den digitalen Wandel und für eine spürbare Verringerung der Steuerbürokratie wird eine zentrale Organisationseinheit auf Bundesebene eingerichtet. …

(S. 167) Wir werden weiterhin den Umsatzsteuerbetrug bekämpfen. Dieser Weg soll in Zusammenarbeit mit den Ländern intensiviert werden. Wir werden schnellstmöglich ein elektronisches Meldesystem bundesweit einheitlich einführen, das für die Erstellung, Prüfung und Weiterleitung von Rechnungen verwendet wird. So senken wir die Betrugsanfälligkeit unseres Mehrwertsteuersystems erheblich und modernisieren und entbürokratisieren gleichzeitig die Schnittstelle zwischen der Verwaltung und den Betrieben. …

(S. 170) Finanzieller Verbraucherschutz und Altersvorsorge: … Wir werden umgehend prüfen, wie die Transparenz beim Kredit-Scoring zugunsten der Betroffenen erhöht werden kann. Handlungsempfehlungen werden wir zeitnah umsetzen. …

(S. 171) Geldwäsche: … Für die laufende Bewertung und Verbesserung der Effektivität der Geldwäschebekämpfung in Deutschland soll die notwendige Informations- und Erkenntnisgrundlage aufgebaut werden. Die Geldwäsche-Meldungen aus dem Nicht-Finanzbereich, wie z.B. dem Immobiliensektor, wollen wir erleichtern und im Vollzug deutlich erhöhen. … Die EU-Aufsichtsbehörde soll sich nicht nur um den klassischen Finanzsektor kümmern, sondern auch den Missbrauch von Kryptowerten für Geldwäsche und Terrorismusfinanzierung verhindern. …

Die FIU muss die notwendigen rechtsstaatlich abgesicherten Befugnisse bekommen sowie den Zugang zu allen nötigen Informationen. Wir werden Verbindungsbeamte aus den Landeskriminalämtern in der FIU einsetzen. Wir wollen den risikobasierten Ansatz weiter verbessern. Ferner wollen wir die Qualität der Meldungen verbessern, indem die Verpflichteten verstärkt Rückmeldung bekommen. …

(S. 172) Wir werden die Qualität der Daten im Transparenzregister verbessern, sodass die wirtschaftlich Berechtigten in allen vorgeschriebenen Fällen tatsächlich ausgewiesen werden. Wir wollen die digitale Verknüpfung mit anderen in Deutschland bestehenden Registern. Wir werden das Datenbankgrundbuch mit dem Transparenzregister verknüpfen, um die Verschleierung der wahren Eigentümer von Immobilien zu beenden. Verknüpfung und Nutzung werden wir datenschutzkonform gestalten. …

Digitale Finanzdienstleistungen und Währungen: Für FinTechs, InsurTechs, Plattformen, NeoBroker und alle weiteren Ideengeber soll Deutschland einer der führenden Standorte innerhalb Europas werden. Es gilt, die mit den neuen Technologien, wie z.B. Blockchain, verbundenen Chancen zu nutzen, Risiken zu identifizieren und einen angemessenen regulatorischen Rahmen schaffen. Wir werden deshalb für effektive und zügige Genehmigungsverfahren für FinTechs sorgen. Digitale Finanzdienstleistungen sollten ohne Medienbrüche funktionieren; dafür werden wir den Rechtsrahmen schaffen und die Möglichkeit zur Emission elektronischer Wertpapiere auch auf Aktien ausweiten. Den Prozess zur Einführung eines digitalen Euro als Ergänzung zum Bargeld, der als gesetzliches Zahlungsmittel in Europa für alle zugänglich und allgemein einsetzbar ist, wollen wir konstruktiv begleiten. Europa braucht zudem eine eigenständige Zahlungsverkehrsinfrastruktur und offene Schnittstellen für einen barrierefreien Zugang zu digitalen Finanzdienstleistungen für alle Verbraucherinnen und Verbraucher sowie Händler.

Wir brauchen eine neue Dynamik gegenüber den Chancen und Risiken aus neuen Finanzinnovationen, Kryptoassets und Geschäftsmodellen. Wir setzen uns für ein Level-Playing-Field mit gleichen Wettbewerbsbedingungen innerhalb der EU, zwischen traditionellen und innovativen Geschäftsmodellen und gegenüber großen Digitalunternehmen ein. Das europäische Finanzmarktaufsichtsrecht machen wir fit für die Digitalisierung und für komplexe Konzernstrukturen, um eine ganzheitliche und risikoadäquate Aufsicht über neue Geschäftsmodelle sicherzustellen. Wir brauchen für den Kryptobereich eine gemeinsame europäische Aufsicht. Wir verpflichten Kryptoassetdienstleister zur konsequenten Identifikation der wirtschaftlich Berechtigten.



Bild: iStock | Todor Dinchev

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Login-Falle statt Klarnamenpflicht

Von diversen Innen- und Sicherheitspolitikern wird immer wieder die Klarnamenpflicht bei der Internetnutzung, insbesondere bei Social Media eingefordert: Jede und Jeder soll online unter dem echten Namen kommunizieren müssen, statt sich hinter einem Pseudonym verstecken zu können. Wie sonst solle man im Kampf gegen Hass und Hetze in sozialen Medien die Identität von beleidigenden, pöbelnden oder drohenden Nutzern feststellen? Der Bundesgerichtshof verhandelt derzeit darüber, ob Facebook berechtigt ist die Accounts von Usern ohne echten Namen zu sperren.

Netzaktivisten kämpfen gegen diese Idee. Henning Tillmann, Co-Vorsitzender des Digitalpolitik-Thinktanks D64, meint, die Klarnamenpflicht „würde die Voraussetzungen für freie Meinungsäußerung einschränken, übrigens nicht nur für Dissidenten und Whistleblower, sondern für uns alle. Es muss die Möglichkeit geben anonym aufzutreten." Eine Klarnamenpflicht komme ähnlich wie die anlasslose Vorratsdatenspeicherung einem Pauschalverdacht gleich, weil sie alle beträfe – und nicht nur die, die potenziell strafrechtlich Relevantes schreiben. Das Gleiche gelte für die „Identifizierungspflicht", mit der Nutzer zwar nicht unter ihrem echten Namen posten, ihn aber bei den Plattformen hinterlegen müssen. Solch eine „Riesensammlung persönlicher Daten bei privaten Konzernen" mache diese zu attraktiven Angriffszielen.

D64 hat deshalb eine Alternative ersonnen, die es auf Seite 109 des Ampel-Koalitionsvertrags geschafft hat: die „Login-Falle". Mit ihrer Hilfe sollen Nutzer Beiträge direkt bei der Polizei anzeigen können. Diese müsste dann prüfen, ob ein Anfangsverdacht auf eine Straftat besteht, und nötigenfalls veranlassen, dass der Plattformbetreiber die Login-Falle scharf stellt: Logt sich der Verfasser dann erneut mit seinem Account ein oder zeichnet die App im Hintergrund weiter Daten auf, wird die IP-Adresse abgefangen. Mit der kann die Polizei vom Telekommunikationsanbieter die Identität erfragen.

Eine solche Login-Falle würde laut Tillmann Datenschutzbedenken ausräumen und nebenbei die heikle Entscheidung, ob ein Beitrag gesetzeswidrig ist oder nicht, von den Plattformbetreibern zum Staat verlagern. Derzeit verpflichtet das Netzwerkdurchsetzungsgesetz (NetzDG) Facebook, Youtube und die anderen Plattformen dazu selbst zu kontrollieren, ob Beiträge womöglich rechtswidrig und zu löschen sind. Damit werde die Durchsetzung des Rechts privatisiert, kritisieren Netzaktivisten.

Laut D64 braucht es für die Login-Falle zwischen den Plattformen und den Strafverfolgungsbehörden standardisierte Schnittstellen für eine schnelle und sichere Übermittlung. Technisch ist das, so D64, machbar. Die Social-Media-Betreiber müssen sowieso von Februar 2021 an mutmaßlich Illegales in schweren Fällen ans Bundeskriminalamt weiterleiten. Bekannt ist auch, dass sie alles andere als glücklich sind über den Kontrollaufwand, den das NetzDG ihnen aufbürdet. Die großen Anbieter, etwa Meta, der neue Facebook-, WhatsApp- und Instagram-Mutterkonzern, oder Google, wozu Youtube gehört, äußerten sich bisher nicht zu den Chancen, den Risiken und zur technischen Umsetzbarkeit einer Login-Falle.

Die Telekom bestätigte, dass für Telekommunikationsunternehmen, die mithilfe der IP-Adresse Namen und Adresse herausgeben müssten, ihr Part der „Falle" recht unkompliziert umsetzbar ist: Schon jetzt gibt es ein standardisiertes Vorgehen, wenn Strafverfolgungsbehörden auf richterlichen Beschluss einen Anschlussteilnehmer ermitteln und dafür eine IP-Adresse überprüfen wollen.

Rechtlich wie technisch müsste geklärt werden, ob die „Falle" auch bei Messenger-Diensten wie Telegram, die ja gerade besonders unter Beobachtung stehen als Sammelplattform für Radikale aller Art, angewendet werden kann. Theoretisch könnten sich Nutzer diverser Plattformen entziehen, indem sie ihre IP-Adressen etwa mit Hilfe eines VPN-Zugangs verschlüsseln oder Wegwerf-Accounts nutzen, die sie nach dem Posten löschen. Das täten allerdings die wenigsten Online-Hetzer, sagt Henning Tillmann. Und selbst diese wenigen machten irgendwann Fehler: „Einen großen Teil würde man erwischen."

Im Sommer 2021 hatten sich die Innenminister der Länder zur Lösung des Hetzproblems für eine Identifizierungspflicht ausgesprochen. Zugleich betonte aber Niedersachsens Innenminister Boris Pistorius (SPD), die Login-Falle könne das überflüssig machen. Der Vize-Fraktionsvorsitzende der Grünen im Bundestag, Konstantin von Notz, erklärte, die Ampelkoalition lehne eine generelle Identifizierung ab. Dagegen könnte die Login-Falle „eine grundrechtschonende Identifizierung der potenziellen Täterinnen und Täter ermöglichen". Die Koalition will hierfür ein „Gesetz gegen digitale Gewalt" auflegen, das Opfern mehr Auskunftsrechte eröffnet. Außerdem sollen Richter Account-Sperren anordnen dürfen. Gemäß von Notz kann die Login-Falle jedenfalls im Kampf gegen Hass und Hetze einer von vielen Bausteinen sein (Koopmann, Login in die Falle, SZ 14.12.2021, 5).

Bund

Debatte über Impfregister nimmt Fahrt auf

Ein zentrales Diskussionsthema des noch jungen Pandemiejahres 2022 ist die Einführung einer generellen Impfpflicht. Sollte diese kommen, stellt sich

gleich die Folgefrage, wie diese kontrolliert und durchgesetzt wird.

- Für ein Register

Der Deutsche Ethikrat hat kurz vor Weihnachten 2021 empfohlen, ein nationales Impfregister einzuführen. Es wäre praktisch die einzige Möglichkeit flächendeckend und umfänglich zu überprüfen, ob eine Impfpflicht eingehalten wird oder nicht, glauben auch viele in Medizin und in Bürokratie kundige Menschen. Eventuell könnte sich sogar ein Impfregister als ein milderes Mittel zu einer Impfpflicht erweisen, wenn hierüber die Impfquote erkennbar erhöht und die Bevölkerung überzeugt werden kann. Über ein Impfregister ließen sich einfach die relevanten Daten speichern und abrufen: Impfstoff, Impfdaten und Chargennummern. Der Impfstand könnte erfasst und ausgewertet werden. Die Menschen könnten automatisch an die nächsten Impfungen erinnert werden.

Bundestagspräsidentin Bärbel Bas (SPD) meinte, eine Impfpflicht ergebe nur mit einem nationalen Impfregister Sinn. Nur so ließen sich Fälschungen vermeiden – und Menschen könnten gezielt für einen Impftermin angeschrieben werden. Der Parlamentarische Geschäftsführer der Unionsfraktion, Thorsten Frei (CDU), hielt ein Impfregister deshalb gar für „zwingend notwendig". Der Bundesbeauftragte für den Datenschutz, Ulrich Kelber, nannte die Einführung eines Impfregisters zumindest grundsätzlich machbar: „Datenschutzrechtlich unmöglich ist ein nationales Impfregister nicht." Es müsste allerdings klar begründet werden, warum man es brauche; die Legitimation falle leichter, wenn es nicht nur um Kontrolle des Einzelnen ginge. Ein „gut ausgeführtes Gesundheitsregister" sei denkbar, schnell zu haben sei es sicher nicht. Der Bundesverband mittelständische Wirtschaft ist dafür.

- Bedenken

Bundesgesundheitsminister Karl Lauterbach (SPD) ist gegen ein Register. Er meint, man könne eine Impfpflicht auch ohne Verzeichnis „monitorieren": „Ich warne davor ein Impfregister zu nutzen. Der Aufbau eines Impfregisters dauert lange und ist auch datenschutzrechtlich nicht unumstritten." Lauterbach strebt eine baldige Einführung einer allgemeinen Impfpflicht an. Der SPD-Politiker meinte jedoch, er wolle dabei ohne „neue Meldestrukturen" auskommen. Zugleich arbeitet das Robert Koch-Institut im Auftrag des Bundesgesundheitsministeriums an Plänen für ein Impfregister zu wissenschaftlichen Zwecken, um etwa einen guten Überblick über Nebenwirkungen zu haben. Lauterbachs Vorgänger, Jens Spahn (CDU), erklärte schon im Mai 2021, es sei ja richtig den Datenschutz ernst zu nehmen, aber der Vorschlag, ein Impfregister einzuführen, sei deshalb leider, leider auf Entrüstung gestoßen.

Baden-Württembergs Datenschutzbeauftragter Stefan Brink warnte vor einem zu großen Zugriff des Staates auf Gesundheitsdaten und der Einführung eines nationalen Impfregisters: „Vorsicht bei nationalen Registern und Finger weg von der Zweckentfremdung von Daten". Rechtlich hält Brink die bundesgesetzliche Einführung eines Registers bei der Zuspitzung der Pandemie und in Folge einer allgemeinen Impfpflicht zwar potenziell für denkbar. Er riet aber davon ab: Bereits jetzt gingen viele Menschen auf die Straße und hätten das Gefühl, der Staat würde sie gängeln: „Das Vertrauen in unseren Staat könnte bei übereilten Schritten weiter sinken. Den Impfstatus ohne Zustimmung der Betroffenen zentral erfassen und auf dieser Basis womöglich Bußgelder verhängen zu wollen, ist eine Vollzugsfantasie, die einen negativen Effekt auf die Impfkampagne haben kann." Die Verwaltung müsste bei einem nicht auf Freiwilligkeit beruhenden Register die vorhandenen Impfdaten erst mal mühsam zusammensuchen, etwa bei den kassenärztlichen Vereinigungen oder bei den Impfzentren.

Brink meinte, dass ein nationales Impfregister nur seinen Zweck erfüllen könne, wenn zugleich die Melderegister zentralisiert oder zumindest zentral abgeglichen würden. Solch ein Schritt sei aus historischen Gründen in Deutschland skeptisch zu sehen. Darüber hinaus würde eine Zentralisierung der regional sehr unterschiedlichen Meldedaten die Verwaltungen erst recht vor große Herausforderungen stellen und dauere nach vorsichtiger Schätzung mindestens ein Jahr. Er empfahl daher, die Einhaltung einer möglichen allgemeinen Impfpflicht stattdessen durch stichprobenhafte Kontrollen sicherzustellen: „Das wäre datenschutzkonform machbar."

- Umsetzungsprobleme

Es würde zweifellos einige Zeit dauern, bis ein eigenes System zur Erfassung der Daten aufgesetzt und angriffs- wie absturzsicher gestaltet ist. Zudem müssten für einen vollständigen Überblick die Daten aller impfpflichtigen Bürger aus den auf Landes- respektive Kommunalebene geführten Melderegistern zusammengetragen werden. Die Digitalisierungsfachleute im Bundesgesundheitsministerium (BMG) gehen davon aus, dass es mindestens ein Jahr dauern würde, ein Impfregister an den Start zu bringen.

Die deutsche Digitalisierungserfahrung zeigt, dass das sogar optimistisch geschätzt sein kann. 2016 etwa beschloss der Bundestag, dass ein Register für Organspender und -empfänger kommen soll. Mehr als fünf Jahre später gibt es das Transplantationsregister immer noch nicht. Andererseits hat es Österreich geschafft, seit Beginn der Pandemie ein Corona-Impfregister aufzubauen; die gesetzliche Grundlage dafür gibt es seit 2012. Nun wird es dazu dienen die ab Februar 2022 geltende Immunisierungspflicht zu überprüfen.

Justizminister Marco Buschmann (FDP) hat den Datenschutz als Argument gegen ein Register aufgeführt. Er sei eben zurückhaltend bei Verzeichnissen mit Daten über die gesamte Bevölkerung. Fachleute sind nicht so pessimistisch (siehe die DVD-Presseerklärung hier im Heft, S. 15).

- Ausgestaltung ist völlig unklar

Dänemark, Finnland, Schweden oder die Niederlande haben schon Impfregister eingeführt, bevor es Covid-19 und Impfpflichtdiskussionen gab. Für Österreich, Dänemark und Schweden gilt die gleiche Datenschutz-Grundverordnung wie für Deutschland. Forscher können dort auf die Registerdaten zugreifen und dadurch sehen, welche Bevölkerungsgruppen besser geimpft sind und

welche schlechter. Ein Punkt, der eng damit zusammenhängt, so Heike Baehrens, gesundheitspolitische Sprecherin der SPD-Bundestagsfraktion: „Unsere bisherigen Informationskampagnen sind sehr breit angelegt. Wir brauchen mehr individuelle Ansprache, Aufklärung und zielgruppenangepasste Beratungsangebote.“ Das würde ein Impfregister „erheblich vereinfachen“. Man könnte zum Beispiel allen Nichtgeimpften einen Brief mit Aufklärung und Terminvorschlägen schicken.

Das sieht auch Virologe Thomas Mertens, Chef der Ständigen Impfkommission (Stiko), so: „Ein zentrales Impfregister hätte aus meiner Sicht Vorteile.“ Damit ermögliche man ein unkompliziertes Impfquotenmonitoring, zudem ließe sich die Schutzwirkung von Impfungen besser erfassen: „Man kann seltene Nebenwirkungen rascher identifizieren.“

In Dänemark ist eine elektronische Patientenakte mit dem Impfverzeichnis verknüpft. So können Forschende prüfen, ob bestimmte Beschwerden vieler Patienten unmittelbar nach einer Impfung aufgetreten sind. In Deutschland erhält das für Arzneimittelsicherheit zuständige Paul-Ehrlich-Institut zwar auch Impfdaten, etwa bei Masern; allerdings melden die Krankenkassen diese Daten in der Regel nur halbjährlich, was für die Corona-Bekämpfung zu langsam ist. Stiko-Chef Mertens erkennt zwar die Bedenken wegen des Aufwands und des Datenschutzes an, doch er sagt, es komme eben von Anfang an auf ein „gutes Konzept“ an. Trotzdem werden die bisher angekündigten Bundestags-Gruppenanträge für eine Impfpflicht wohl kein Register vorsehen.

Unklar bleibt so, wie eine Impfpflicht überprüft werden kann. Justizminister Buschmann hält stichprobenartige Kontrollen für das Wahrscheinlichste. Gerd Landsberg, Hauptgeschäftsführer des Deutschen Städte- und Gemeindebunds, hält davon nicht viel. Die kommunalen Ordnungsämter könnten schon helfen, aber sie arbeiteten schon jetzt „an der Belastungsgrenze“. Voraussichtlich würde auch die Ausfertigung der Bußgeldbescheide auch bei Städten und Gemeinden hängen bleiben. Den Vorschlag von FDP-Politiker Konstantin Kuhle, dass die Einwohnermeldeämter allen Bürgerinnen und Bürgern eine Impfeinladung schicken könnten, unabhängig vom Impfstatus (den kennt ja keiner), lehnt Landsberg ab. Die Kommunen könnten keine weiteren Aufgaben, etwa die Versendung von 83 Millionen Briefen, übernehmen. Es gebe „wirksame Instrumente zur einfacheren Handhabung: Dazu zählt ohne Frage ein nationales Impfregister.“

SPD-Gesundheitspolitikerin Baehrens fordert, dass man sich wenigstens eine Alternative zur Erfassung des Impfstatus überlege, wenn am Ende wirklich kein Impfregister kommt. Dies müsse „möglichst niedrigschwellig digital und eher dezentral“ sein. Beispielsweise anonymisiert über die Corona-Warn-App. Nicht vorrangig, um die Einhaltung einer Impfpflicht zu kontrollieren, sondern, um bisher ungeimpfte Menschen zielgenau ansprechen zu können (Koopmann, Ein Register muss her, Mehr als Kontrolle, SZ 22./23.01.2022, 4, 7; Berner/Gupta/Feldenkirchen/Garbe u.a., Koalition der Wackligen, Der Spiegel Nr. 3 v. 15.01.2022, 14; Preker, Datenschutzbeauftragter warnt vor zu großem Staatszugriff, www.spiegel.de 06.01.2021).

Bund

eID auf dem Smartphone ist jetzt möglich

Die Bundesnetzagentur (BNetzA) hat eine Mitteilung in ihrem Amtsblatt veröffentlicht, dass eine Personenidentifizierung mit einem mobilen Endgerät, bei der ein qualifiziertes Sicherheitszertifikat auf Basis der mit dem Personalausweis verknüpften elektronischen Identität (eID) zum Einsatz kommt, ab sofort prinzipiell rechtlich abgesichert auch bei staatlichen Diensten durchführbar ist. Der Bundestag hatte bereits im Mai 2021 ein Gesetz beschlossen, wonach die Bundesbürger den offiziellen Online-Ausweis direkt in ihrem Smartphone oder Tablet speichern können. Voraussetzung dafür ist, dass sie eines der wenigen technisch dafür bereits geeigneten Mobilgeräte besitzen. Ein Smartphone benötigt für das Verfahren eine eingebettete Sicherheitsarchitektur auf hohem Niveau. Momentan leisten dies auf Basis des staatlich geförderten Projekt Optimos 2.0 vor allem Samsung-Geräte der Reihe Galaxy S20.

Die Regulierungsbehörde hat das eID-Verfahren als „innovative Identifizierungsmethode“ im Einklang mit dem schon 2017 verabschiedeten Gesetz zur Umsetzung der eIDAS-Verordnung der EU anerkannt. Dieser Schritt erfolgte laut der BNetzA „im Einvernehmen“ mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Der Bundesdatenschutzbeauftragte Ulrich Kelber sei dazu angehört worden. Die Verfügung ist zunächst bis zum 21.12.2023 befristet. Verlängert hat die Behörde zugleich Verfügungen zur Online-Identifizierung per Videoübertragung (Video-Ident).

Das Onlinezugangsgesetz (OZG) verpflichtet Bund und Länder, ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten. Gemäß der BNetzA ist die Identifizierung von Antragstellern dabei ein wichtiges Element. Durch Änderungen im Personalausweisgesetz, im eID-Karte-Gesetz und im Aufenthaltsgesetz sei der Ansatz mit einem mobilen Endgerät grundsätzlich zulässig. Dies gelte nun auch für „qualifizierte Vertrauensdienste“.

Bisher wird der elektronische Identitätsnachweis durch zwei Faktoren gewährleistet: Das Wissen der sechsstelligen Geheimnummer und den Besitz von Personalausweis, eID-Karte oder elektronischem Aufenthaltstitel. Mit der Gesetzesreform ist das Smartphone samt der staatlichen AusweisApp2 als „Besitzelement“ dazugekommen. Die Daten für den Ausweisvorgang sind demnach in einem sicheren Verfahren aus dem Speicher- und Verarbeitungselement des Endgeräts zu transferieren.

Das Bundeswirtschaftsministerium fördert zudem bis zu vier große IT-Projekte im „Schaufenster Sichere Digitale Identitäten“, um die Möglichkeiten einer digitalen Ausweisfunktion auf Mobiltelefonen neuerer Generationen zu demonstrieren. Weitere Varianten sind in Planung, verzögern sich aber wie im Fall der im September 2021 gestoppten „ID Wallet“. Probleme gibt es auch beim parallel von der Bundesregierung verfolgten Projekt „Smart eID“ (s.u.). Die Bundesdruckerei verweist darauf, dass die nötigen Sicherheitselemente wie

ein integriertes „Secure Element" oder die eSIM-Karte prinzipiell „keine Einschränkung von Smartphones" vornähmen. Die Technologie sei grundsätzlich breit anwendbar, Gerätehersteller und Mobilfunkanbieter müssten aber die Nutzung ermöglichen. Der BNetzA zufolge steht Verbrauchern generell „ein Bündel an komfortablen Identifizierungsmöglichkeiten zur Verfügung, aus denen je nach Zielgruppe und Anwendung gewählt werden kann" (Krempl, Identitätsnachweis: Online-Ausweisen mit dem Handy jetzt offiziell möglich, www.heise.de 22.12.2021, Kurzlink: https://heise.de/-6305750).

Bund

Projekte „ID-Wallet" und „Smart-E-ID" sind gefährdet

Die alte Bundesregierung wollte Führerschein und Personalausweis aufs Smartphone bringen, doch sind die Prestigeprojekte „ID Wallet" und „Smart-E-ID" in Gefahr. Noch drei Tage vor der Bundestagswahl im September 2021 stellte der damalige Noch-Verkehrsminister Andreas Scheuer als echtes „Zukunftsprojekt" den Führerschein fürs Smartphone vor. Doch die App, auf der man ihn hätte speichern sollen, verschwand kaum eine Woche später wieder aus den App-Stores wegen Sicherheitsmängeln und Überlastung. Auch der Personalausweis fürs Smartphone hätte längst da sein sollen. Mit den beiden Prestigevorhaben wollte die Groko auf ihren letzten Metern zeigen, dass es endlich vorangeht mit der Digitalisierung in Verwaltung und Bürgeralltag. Doch die Projekte sind – vielleicht rettungslos – festgefahren.

Der Führerschein fürs Handy war im Rahmen des Pilotprojekts für das „ID Wallet" vorgesehen, einer elektronischen Brieftasche, in der Nutzer verifizierte Identitätsnachweise speichern können. Die Daten sollten fälschungssicher in einer Blockchain-Datenbank lagern. Erprobt wurde das ID Wallet in drei Hotelketten beim papierlosen Check-in. Nach außen kommunizierten die Verantwortlichen, dass alles funktioniert.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) kam dagegen in einem Bericht, der erst Monate später publik wurde, zu dem Ergebnis, dass die Blockchain-Technologie eine „grundsätzliche Anfälligkeit für Sicherheitslücken des gesamten Systems" birgt, und das „bei unklarem Nutzen". Zudem sei die App „nicht für einen über den Piloten hinausgehenden Betrieb geeignet". Doch das verantwortliche Bundeskanzleramt machte weiter und holte das Verkehrsministerium dazu. Ende September 2021 ging das ID Wallet online.

Bald darauf kritisierte die IT-Sicherheitsexpertin Lilith Wittmann, dass Kriminelle leicht an die sehr sensiblen Nutzerdaten hätten gelangen können. Dazu kam die Überlastung der App-Server durch hohe Nutzerzahlen – offiziell der Hauptgrund, weshalb die App so schnell wieder offline ging. Wittmann: „Es wirkte, als wollte die alte Regierung auf Teufel komm raus noch schnell irgendwas Digitales machen, hat das aber nicht wirklich durchdacht." Direkt nach dem Reinfall hieß es noch, die App sei „in wenigen Wochen" wieder verfügbar. Anfang 2022 teilte ein Regierungssprecher mit, man arbeite mit beteiligten IT-Unternehmen „unter Hochdruck" an Lösungen. Ein konkreter Zeitplan hin zu einem Relaunch „im Jahr 2022" stehe wegen des Regierungswechsels aber noch aus.

Anke Domscheit-Berg, die netzpolitische Sprecherin der Linken-Bundestagsfraktion, erklärte dazu: „Die Ampel-Koalition wäre gut beraten das Projekt in seiner bisherigen Form zu beerdigen". Der Bedarf nach sicherer Identifizierung via Smartphone sei dringend. Doch hält sie die beiden Projekte der alten Koalition, also auch den Smartphone-Personalausweis, für einen „Schuss in den Ofen".

Bei der sogenannten Smart-E-ID für den Personalausweis scheint jedoch mehr Vorsicht zu walten. Das BSI verlangt für die Speicherung einen speziellen Sicherheitschip, der bislang nur in Smartphones der Galaxy-S20-Reihe vom Projektpartner Samsung steckt. Zwar läuft die „AusweisApp2" auf den Geräten, aber nutzbar ist der Ausweis noch nicht. Dabei sollte das schon 2020 möglich sein; später verschob Samsung den Start auf Herbst 2021. Jetzt teilt das zuständige Bundesinnenministerium auf Anfrage mit, es seien „umfangreiche Tests und Abnahmen notwendig", man strebe einen „zeitnahen Starttermin" an, den Samsung-Handys sollten „schnell" weitere Geräte folgen. Die Ampel-Koalition kann zwar einerseits die Verantwortung auf die Vorgängerregierung abwälzen, doch hat sie sich die Digitalisierung prominent auf ihre Fahnen geschrieben. Maximilian Funke-Kaiser, digitalpolitischer Sprecher der FDP im Bundestag, wünscht sich, dass beide Projekte noch realisiert werden: „Durch rein digitale Dokumente können Dienstleistungen und Vorgänge automatisiert werden. Das wäre ein enormer Schritt nach vorne für unsere Gesellschaft."

Der Hauptgeschäftsführer des Digitalverbands Bitkom, Bernhard Rohleder, kritisierte, Deutschland verliere hier wertvolle Zeit. Man solle sich ein Beispiel an Dänemark nehmen, wo neun von zehn Bürgern digitale Identitätsnachweise nutzten. Auch der Deutsche Städte- und Gemeindebund hält es im Zuge der Verwaltungsdigitalisierung für zwingend nötig, dass sich Bürgerinnen und Bürger digital ausweisen können.

IT-Expertin Wittmann verweist derweil auf einen Service, den es schon seit Jahren gibt: die Online-Funktion des herkömmlichen Personalausweises. Nur haben die laut E-Government-Monitor 2021 bloß 9% der Befragten je genutzt. Wittmann sagt, es gebe kaum Anreize für Unternehmen damit die Identität ihrer Kunden zu prüfen: „Die Bundesregierung sollte lieber darin investieren die bestehende Funktion attraktiver und flexibler zu gestalten statt Geld in Technologien zu pumpen, die eigentlich überflüssig wären." Die Idee des ID Wallets klingt zwar praktisch, aber selbst wenn man irgendwann seinen Führerschein in die elektronische Brieftasche hochladen kann, muss man bei Polizeikontrollen nach geltender Rechtslage noch den alten Lappen oder die Plastikkarte vorzeigen (Koopmann, SZ 08./09.01.2022, 7).

Bund

Start eines auszubauenden Lobbyregisters

Nach jahrelangen kontroversen Diskussionen ging am 01.01.2022 das neue Lobbyregister für mehr Transpa-

renz im politischen Entscheidungsprozess an den Start. SPD und Grüne im Bundestag verwiesen derweil auf entsprechende Vereinbarungen im Koalitionsvertrag, wonach dieses schon bald nachgeschärft werden soll. So erklärte die Grünen-Fraktionsvorsitzende Britta Haßelmann: „Mit dem parlamentarischen Verfahren sollten wir möglichst bald beginnen.“ Der Vizevorsitzende der SPD-Fraktion, Dirk Wiese, sekundierte, man wolle dies „gemeinsam zeitnah auf den Weg bringen“. Auch die Organisation Transparency International mahnte Nachbesserungen an.

Das öffentlich einsehbare Lobbyregister soll sichtbar machen, wer Einfluss auf politische Entscheidungen und die Gesetzgebung nimmt. Professionelle Interessenvertreter sind nun verpflichtet sich dort bis spätestens 01.03.2022 einzutragen. Sie müssen Angaben unter anderem über ihre Auftraggeber und zum personellen und finanziellen Aufwand ihrer Lobbytätigkeit bei Bundestag und Bundesregierung machen. Zu erläutern sind auch der Interessenbereich und die Tätigkeit. Treffen in Ministerien sollen bis zur Ebene von Unterabteilungsleitern erfasst werden.

Lobbyisten werden zudem verpflichtet sich an einen Verhaltenskodex zu halten. So soll ihre Tätigkeit „auf der Basis von Offenheit, Transparenz, Ehrlichkeit und Integrität“ erfolgen. Informationen dürfen niemals auf unlautere Art und Weise – insbesondere durch finanzielle Anreize – beschafft werden. Unzulässig sind auch Vereinbarungen, durch die eine Vergütung oder deren Höhe vom Erfolg der Interessenvertretung abhängig gemacht wird. Lobbyisten, die sich nicht an die Regeln halten, droht ein Bußgeld von bis zu 50.000 Euro.

Bundestagspräsidentin Bärbel Bas (SPD): „Ich bin stolz auf den Startschuss. Künftig kann jeder im Lobbyregister nachlesen, welche Interessenvertreter in welchen Politikfeldern unterwegs sind, wer ihre Auftraggeber sind und wie viel Geld dafür ausgegeben wird.“ Auch Bas meinte, ein Nachschärfen der Regeln könnte nötig werden. Solche Nachbesserungen fordert die Organisation Transparency International. Sie verlangt insbesondere die Einführung eines „legislativen Fußabdrucks“, also einen Hinweis in allen neuen Gesetzen, welche Interessenvertreter darauf Einfluss genommen haben. Zwar habe die Ampel-Koalition vereinbart diesen nachträglich einzuführen, sagte der Vorsitzende von Transparency Deutschland, Hartmut Bäumer: „Aber da kommt es darauf an, wie es aussieht. Das werden wir uns genau angucken.“ „Völlig unverständlich“ seien die Ausnahmen für Kirchen, Gewerkschaften und Kommunalverbände.

Für eine Fehlkonstruktion hält es Transparency, dass das Register dem jeweiligen Bundestagspräsidenten oder der -präsidentin unterstellt ist, so Bäumer: „Es muss eine neutrale Instanz geben wie beim Datenschutzbeauftragten, die nicht weisungsabhängig ist“. Dort solle das Register geführt und die Einhaltung der Regeln kontrolliert werden. „Es muss eine Institution sein, die auch ein bisschen Biss hat.“

Grünen-Fraktionschefin Haßelmann begrüßte den Start des Lobbyregisters. Die große Koalition habe auf hohen Druck der Öffentlichkeit und der Opposition hin erste Schritte für mehr Transparenz gemacht, die jedoch nicht weit genug gingen. „Jetzt haben Grüne, SPD und FDP vereinbart das Lobbyregister nachzuschärfen und so für mehr Transparenz zu sorgen.“ Neben der Einführung des „Fußabdrucks“ sei geplant den Kreis der registrierten Interessensvertreterinnen und -vertreter zu erweitern und die Schwelle für anzugebende Kontakte in den Ministerien bis auf die Referentenebene zu senken.

Das Lobbyregister wird digital beim Bundestag geführt. Dort rechnet man mit einer Größenordnung von 6.000 bis 8.000 Interessenvertretern, die sich anmelden werden. Zum Vergleich: Die bisherige öffentliche Liste der beim Bundestag registrierten Verbände, die mit dem neuen Register obsolet wird, enthält gerade einmal 2.238 Einträge. Die DVD hat sich im neuen Lobbyregister angemeldet. Ihr Eintrag ist zu finden unter https://www.lobbyregister.bundestag.de/suche/R000173/ (Steinkohl, Lobbyregister geht an den Start: rasche Nachschärfung geplant, www.heise.de 30.12.2021, Kurzlink: https://heise.de/-6315112; Lobbyregister startet, SZ 31.12.2021-02.01.2022, 8, vgl. DANA 2/2021, 110 f.).

Bund

Pränataler Gentest als Kassenleistung

Der vorgeburtliche genetische Test auf die Trisomien 13, 18 und 21 kann ab Frühjahr 2022 auf Kosten der Gesetzlichen Krankenversicherung in Anspruch genommen werden. Der Gemeinsame Bundesausschuss (G-BA) bereitete dafür auf seiner Sitzung am 19.08.2021 den Weg, indem die Versicherteninformationen zum Nicht-invasiven Pränataltest (NIPT) sowie dem Leben mit einem Kind mit Trisomie verabschiedet wurden. Damit tritt auch der Beschluss der Kassenfinanzierung vom September 2019 in Kraft. Zur rechtsaufsichtlichen Prüfung wurde die Versicherteninformation dem Bundesministerium für Gesundheit vorgelegt und nicht beanstandet (GiD Nr. 259 November 2021, 28).

Bundesweit

Corona-Gästedaten für strafrechtliche Ermittlungen genutzt

Eine bundesweite Umfrage des ZDF unter allen deutschen Staatsanwaltschaften und Landesdatenschutzbeauftragten ergab, dass Polizeien und Staatsanwaltschaften häufig auf personenbezogene Daten zur Corona-Kontaktnachverfolgung zugegriffen haben. Seit Einführung des Erfassungssystems in Gastronomie, Freizeiteinrichtungen und Geschäften im Frühsommer 2020 sollen Strafverfolgungsbehörden in mehr als 100 Fällen Informationen wie Namen, Anschriften, Telefonnummern und E-Mail-Adressen aus Papier-Kontaktlisten sowie zumindest in einem Fall aus der Luca-App erhoben haben. Betroffen von den umstrittenen Aktionen waren demnach mindestens 500 Personen. Der Sender geht von einer hohen Dunkelziffer aus: Derartige Datenabfragen würden bei den Staatsanwaltschaften nicht gesondert erfasst, so dass die Zahlen vor allem auf der Erinnerung der Beamten beruhten. Zudem habe die Polizei Informationen teils ohne

Wissen der Staatsanwaltschaften erhoben.

In mindestens fünf Fällen sind dem Bericht zufolge die Daten abgefragt worden, obwohl das Infektionsschutzgesetz des Bundes (IfSG) dies zu diesem Zeitpunkt bereits untersagte. § 28a IfSG verbietet eine Nutzung der Informationen „zu anderen Zwecken als der Kontaktnachverfolgung". Ob diese Formulierung ohne jede Ausnahme auch für die Aufklärung schwerster Straftaten wie Mord gilt, ist rechtlich umstritten. Der bayerische Datenschutzbeauftragte Thomas Petri hält die Informationen grundsätzlich für tabu.

Ein bekannter Fall war der Zugriff der Mainzer Polizei auf Luca-Daten über einen Trick des Gesundheitsamts bei Ermittlungen zu einem Sturz mit Todesfolge in der Altstadt der Landeshauptstadt (s.u. S. 38). Laut ZDF fragten unter dem überarbeiteten IfSG auch Strafverfolgungsbehörden in Mosbach, Koblenz, Stuttgart und Oldenburg Kontaktdaten ab, die in diesen Fällen nicht über Luca erfasst wurden. Sie ermittelten dabei unter anderem wegen eines Tötungsdelikts sowie des Verdachts des sexuellen Kindesmissbrauchs.

Bevor es die Luca-App und vergleichbare Systeme gab, hatte die Polizei in mehreren Bundesländern ebenfalls bereits auf personenbezogene Daten aus Corona-Gästelisten von Restaurants, Cafés und Hotels zugegriffen. Bayerische Ordnungshüter gingen damit sogar gegen Kleinkriminalität vor. Damals hatte die Rechtslage noch mehr Interpretationsspielraum gelassen (DANA 4/2020, 247, 3/2020, 187 f.). Ein Sprecher des Bundesdatenschutzbeauftragten Ulrich Kelber empfahl besser auf die Check-in-Funktion der Corona-Warn-App (CWA) zu setzen. Damit stehe eine Lösung bereit, „bei der aufgrund des dezentralen Ansatzes eine unerlaubte Datenabfrage nicht möglich ist". Die Anwendung des Robert-Koch-Instituts sei bisher aber nur in wenigen Bundesländern gesetzlich zur Kontakterfassung als Alternative erlaubt. Auch der Bundestag empfiehlt zu diesem Zweck die CWA (Krempl, Luca und Listen: Polizei hat in über 100 Fällen Kontaktdaten abgefragt, www.heise.de 21.01.2021, Kurzlink: https://heise.de/-6335124).

Bundesweit

Initiative „Datenschutz geht zur Schule" – Bundesweiter Kreativwettbewerb an Schulen

Bis Ende April 2022 schreibt die Initiative des Bundesverbands der Datenschutzbeauftragten Deutschlands (BvD) bundesweit einen Wettbewerb für Schülerinnen und Schüler aus. „Datenschutz geht zur Schule" (DSgzS) möchte mit dem Wettbewerb den Datenschutz, der für die junge Generation „eher uncool" zu sein scheint, beleben. Ob Sprüche, Icons oder andere Ideen: Was von der Jury (Morpheus, Shary Reeves, Steven Gätjen und TotallyGamerGirl) prämiert wird, soll veröffentlicht und als Aufkleber in großer Auflage als Give-aways produziert werden. Der Sprecher der Initiative betont, es gehe „um Aufmerksamkeit für das wichtige Thema Datenschutz, das Rüsten der jungen Generation mit Medienkompetenz und für Lehrkräfte um einen spielerischen Einstieg in ein topaktuelles Themengebiet". Die Initiative DSgzS wurde im letzten Jahr im DANA-Schwerpunktheft „Bildung" 2/2021, 85 ff. ausführlich vorgestellt (www.bvdnet.de/kreativpreis).

Bundesweit

Gesetze zur Ernennung von Datenschutzbeauftragten verstoßen gegen DSGVO

Ein aktuelles Gutachten des Netzwerks Datenschutzexpertise zur Bestellung öffentlicher Datenschutzbeauftragter kommt zu dem Ergebnis, dass der Auswahlprozess der Landesbeauftragten und der Bundesbeauftragten für Datenschutz noch immer weitgehend gegen die Vorgaben der europäischen Datenschutzgrundverordnung (DSGVO) verstößt. Ende 2021 waren zwei Leitungen von Aufsichtsbehörden seit Monaten unbesetzt. 2022 stehen in sechs Bundesländern Wieder- bzw. Neubesetzungen an.

Das vom Datenschutzexperten Thilo Weichert erstellte Gutachten stellt heraus, dass die Auswahl der Leitungsposition der Datenschutzaufsichtsbehörden hinsichtlich ihrer „grundrechtlichen, rechtsstaatlichen und demokratischen" Bedeutung sehr wichtig ist: „Mit ihrer Unabhängigkeit sollen sie angesichts der besonderen grundrechtlichen Risiken einen frühzeitigen, effektiven, vorgezogenen Rechtsschutz gewähren."

Gemäß dem Gutachten stimmen Qualifikationskriterien und Auswahlprozesse in der Praxis in vielen Ländern und im Bund nicht mit den Vorgaben der DSGVO überein, die seit 2018 umgesetzt sein müssten. Artikel 53 DSGVO verlangt, dass die Behördenleiter über „erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen" müssen. In Hamburg beispielsweise trat in diesem Jahr ein Spezialist für Medienrecht die Nachfolge von Johannes Caspar an. Die jüngst von ihrem Amt zurückgetretene Berliner Datenschutzbeauftragte Maja Smoltczyk hatte vor ihrem Amtsantritt nur marginal mit Datenschutz zu tun, ebenso die viel kritisierte ehemalige Bundesdatenschutzbeauftragte Andrea Voßhoff.

Die Auswahl der Kandidaten muss gemäß dieser Regelung in einem „transparenten Verfahren" erfolgen: „Die Kräfte, die auf die Bestellung der Mitglieder Einfluss nehmen, müssen so ausbalanciert werden, dass keine einseitige Einflussnahme stattfindet", so das Gutachten. Es müsse „verhindert werden, dass Personen in das wichtige öffentliche Amt gelangen, ohne dass es zuvor eine öffentliche Debatte gibt, bei der die geforderte Balance erzielt werden kann." Das ist offenkundig nicht der Fall, wenn die Regierungen Verwaltungsjuristen, die etwa im Innenministerium arbeiteten, für die Leitung der unabhängigen Datenschutzaufsichtsbehörden vorschlagen.

Angesichts der einheitlichen Vorgaben der DSGVO sei es „verwunderlich", wie unterschiedlich der Auswahlprozess und die Amtsdauer in Deutschland geregelt sind. Die gesetzlich vorgesehenen Amtszeiten reichen von fünf bis acht Jahre. Die Wiederwahl ist etwa in Baden-Württemberg zweimal möglich, in vielen Bundesländern nur einmal. In Bayern oder Hessen gibt es keinerlei Beschränkungen. Eine Ausschreibungspflicht gibt es nur in Sachsen-Anhalt – doch in der Praxis wurde sie noch nicht

umgesetzt: 2017 hätte der Landtag einen Nachfolger von Harald von Bose wählen müssen. Per Gesetz endete seine Amtszeit Ende 2020. Seither ist die Stelle unbesetzt. Auch in Berlin ist sie unbesetzt. In NRW war die Stelle vom Sommer 2020 bis Frühjahr 2021 ohne Besetzung.

Das Vorschlagsrecht steht in vier Bundesländer sowie dem Bund der Regierung zu, ansonsten erfolgen die Vorschläge aus dem Parlament beziehungsweise den Regierungsfraktionen. Gewählt wird dann durchgängig in den Parlamenten – mit Ausnahme des Präsidenten des Bayerischen Landesamts für Datenschutzaufsicht, der von der Staatsregierung benannt wird. Eine Aussprache über die Kandidaten ist in sechs Parlamenten ausdrücklich ausgeschlossen. In den weiteren elf Parlamenten wurde von der Möglichkeit noch nie Gebrauch gemacht.

Die Ernennungsverfahren hält das Gutachten in Summe für „defizitär", da die Transparenz des Verfahrens kaum oder gar nicht gewährleistet sei. Außerdem wird darin kritisiert, dass die Wiederbesetzung offener Stellen immer wieder verzögert wird. Das Gutachten erinnert daran, dass vor 2018 immer wieder „sachfremde Erwägungen" bei der Besetzung der Stellen ausschlaggebend waren: Parteibuch und Ämterpatronage seien wichtiger gewesen als die fachliche Qualifikation. Seither seien „offensichtlich unqualifizierte" Ernennungen nicht mehr zu beobachten. In Schleswig-Holstein gab es 2020 sogar erstmals den Versuch gegen die Ernennung gerichtlich vorzugehen, da keine Ausschreibung erfolgt war. Das hatte jedoch vor dem Verwaltungsgericht Schleswig keinen Erfolg.

Als Fazit stellt das Gutachten fest, dass die Transparenz idealerweise über eine Ausschreibung hergestellt werden könne, die gesetzlich festgeschrieben werden sollte. Da die Qualität der Leitung durch den Auswahlprozess „stark bestimmt" werde, sei die Etablierung „professioneller Abläufe notwendig": Die „weithin verbreitete politische Praxis des Ausklüngelns in Hinterzimmern" müsse beendet werden.

Die Datenschutzkonferenz von Bund und Ländern hat sich bislang zu der Problematik nicht geäußert. Der Jurist Malte Engeler, der in einem intransparenten Auswahlprozess in Hamburg scheiterte, meint: „Derzeit starten die neu ernannten Amtsleitungen aber mit einer völlig unnötigen und vermeidbaren Hypothek auf ihre Glaubwürdigkeit." Der baden-württembergische Datenschutzbeauftragte Stefan Brink, der 2022 zur Wiederwahl ansteht, sieht in einer Ausschreibung einen Vorteil für den Amtsinhaber: „Nur wer aus einem transparenten und qualifizierten Auswahlverfahren erfolgreich hervorgeht, kann die mit dem Amt verbundenen Pflichten an Sachkunde und persönlicher Unabhängigkeit erfüllen."

Die schleswig-holsteinische Landesdatenschutzbeauftragte Marit Hansen, deren Wiederwahl vor Gericht angefochten wurde, sagte: „Ich persönlich befürworte Ausschreibungen, weil dies zur Bewerbung ermutigen kann. Selbst bin ich ja auch über eine Ausschreibung und mehrere Auswahlgespräche in das Amt gekommen." Möglich war das, weil die Piraten sich damals im Landtag für dieses Vorgehen eingesetzt hatten. Rechtlich ist eine Ausschreibung nach Auffassung des Verwaltungsgerichts Schleswig derzeit nicht vorgeschrieben. Aus eigener Erfahrung fügt Hansen hinzu: „Aber auch Ausschreibungen verhindern nicht, dass jemand bei den Wahlberechtigten vorab Strippen zieht, auf sein Parteibuch pocht oder Rufschädigungen bezüglich einer anderen Person betreibt" (Schulzki-Haddouti, Gutachten: Auswahlverfahren für Datenschützer verstößt gegen DSGVO, www.heise.de 03.12.2021, Kurzlink: https://heise.de/-6283293, Netzwerk Datenschutzexpertise, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2021_bestellgbfdilfd03.pdf).

Bundesweit

Marktplätze von Otto & Co. verweigern Verantwortung für Datenleck

Informationen, z.B. Bestellungen, Adressen und auch Kontodaten, über Nutzende der großen Onlinemarktplätze Otto, Kaufland (ehemals real), Mediamarkt, Check24, Tyre24, idealo, Hood und Crowdfox waren wegen Sicherheitsmängeln des Dienstleisters „Modern Solution" für Dritte abrufbar. Die Marktplätze verweigern sich jedoch ihrer datenschutzrechtlichen Verantwortlichkeit. Von dem Datenleck betroffen waren rund 700.000 Endkunden. Von ihnen ließen sich Transaktionen seit dem Sommer 2018 einsehen: wer wann was von welchem Händler gekauft hat, mitsamt Anschrift, und in mehreren Tausend Fällen sogar die dazugehörigen Bankverbindungen.

Nach Bekanntwerden des Leck erklärte ein Otto-Sprecher, der Vorfall werde „zum Anlass genommen den gesamten Prozess infrage zu stellen" und ihn eventuell zu überarbeiten. Die Zugänge der Händler zum Marktplatz wurden komplett gesperrt. Ähnlich reagierte eine Sprecherin von Check24. Man verwende bei den betroffenen Shopping-Angeboten generell Alias-E-Mails für bestellende Kunden, die echten Maildaten würden nicht an die Händler weitergegeben, ebensowenig Bankdaten. So sollten die Kundeninformationen geschützt werden. Kaufland wiederum betont nur E-Mails und die Anschrift der Kunden bei einer Bestellung weiterzugeben.

- Fehlerquelle: IT-Dienstleister

Das Datenleck entstand bei dem Dienstleister Modern Solution, über den Einzelhändler sich an die Schnittstellen der Marktplätze im Web anbinden lassen. Solche Firmen sind eine Art technischer Mittler zwischen Händlern und Online-Handelsplattformen. Eine förmliche Vertragsbeziehung haben daher nur die Händler mit dieser Firma, nicht aber die Marktplätze selbst. Die Plattformen schreiben Händlern zwar vor sich um die Sicherheit der Daten zu kümmern, mehr aber auch nicht. Bei Kaufland hieß es, bei einer Bestellung seien die Händler direkte Vertragspartner der Kunden und damit für den Schutz der Kundendaten verantwortlich. Und der Otto-Sprecher ergänzte, man wolle die Kundendaten schützen: „Ein solcher Vorfall, hervorgerufen durch einen Dritten, zu dem wir keine Vertragsbeziehung unterhalten, ist dann sehr schädlich."

Ca. ein Dutzend solcher Schnittstellendienstleister tummelten sich

im deutschen Markt. Sie helfen den Händlern, die sich nicht direkt selbst an die Plattformen anbinden wollen oder können, und verknüpfen dabei die Schnittstellen der Plattformen mit den jeweiligen Warenwirtschaftssystemen der Händler, die ihre Waren über die Onlinemarktplätze verkaufen wollen. Bei dem Datenleck von Modern Solution zeigt sich, wie sorglos dabei teils mit den Kundendaten umgegangen wird.

Als ein IT-Spezialist im Juni 2021 im Auftrag eines Einzelhändlers bei der Anbindung zu dessen Schnittstellendienstleister Modern Solution ein technisches Problem beseitigen sollte, stieß er auf die klaffenden Sicherheitslücken. Modern Solution gewährte seinen Kunden demnach einen direkten Zugriff auf seinen Server und mehrere dort hinterlegte Datenbanken. Die Firma aus Gelsenkirchen hatte zudem in ihrer Software, die jeder Händler bei sich installieren muss, problemlos auslesbare Zugangsdaten zu diesem Server hinterlegt, und die galten gleichermaßen für alle Kunden. Die Folge: Ein Kunde von Modern Solution konnte auf dem Server des Dienstleisters die Datenbanken aller anderen Kunden und die Transaktionen von deren Endkunden einsehen. All diese Informationen lagen dadurch praktisch offen vor dem IT-Spezialisten.

Der IT-Spezialist, Chef eines Dienstleisters für Onlinehändler, erläuterte: „Man muss sich vorstellen, da ist ein Programm, das alle Daten aller Händler und von deren Marktplätzen aggregiert. Und dann hatten die für ihre Datenbanken das Passwort im Klartext und ohne Verschlüsselung hinterlegt, Kundendaten obendrein auf dem Server seit Jahren nicht gelöscht.“ Die Software mit den Händlerzugangsdaten bei Modern Solution hätte man seinen Angaben zufolge theoretisch auch über eine Google-Suche finden können, da es für die entsprechende Datei einen freien Downloadlink gab. Den Modern-Solution-Server wiederum könnten automatisierte Suchprogramme finden. Ob das irgendwann mal irgendjemand ausgenutzt hat, ist unklar. Modern Solution schrieb in seiner ersten Stellungnahme an seine Kunden, das sei „derzeit nicht bekannt“.

Die praktisch nicht existente Trennung bedeutete zudem, dass ein Händler, wenn er gehackt worden wäre, zum Sicherheitsrisiko für alle anderen Kunden des Dienstleisters geworden wäre. Anonym warnte der IT-Experte nach seiner Entdeckung Modern Solution in einer E-Mail: Mit Erschrecken habe er festgestellt, „dass die übermittelten Zugangsdaten zu mehreren Datenbanken auf Ihren Servern führen“. In den Datenbanken befänden sich „empfindliche benutzerbezogene Daten“. Weitere Kundendaten ließen sich aus anderen Tabellen auslesen. Er wandte sich auch an Mark Steier, den Betreiber der auf Onlinehandel spezialisierten Website wortfilter.de. Steier veröffentlichte am 23.06.2021 einen ersten Artikel zu dem Fall, danach mehrere weitere, auch weil die ersten eiligen Reparaturversuche von Modern Solution offenbar untauglich waren.

Das bestätigen auch Aussagen eines Unternehmenssprechers von Otto. Sofort nach Bekanntwerden des Vorfalls seien alle Passwörter der Händler zurückgesetzt worden: „Als Modern Solution vorgab die Sicherheitslücke gefixt zu haben, stellten wir fest, dass das System weiterhin unsicher war.“ Daraufhin seien die Zugänge dann komplett gesperrt worden und eine Anbindung an den Shop für Händler nur noch direkt möglich gewesen. Darüber seien die Händler informiert worden. Die Website von Modern Solution wurde durch einen „Liveticker“ ersetzt, in dem die Firma ihre Umbaumaßnahmen dokumentierte.

- Onlinemarktplätze entziehen sich Verantwortung

Für die Einzelhändler ist der Vorgang problematisch, weil sie verstärkt auf die Onlinemarktplätze streben, um sich vom schwieriger werdenden Geschäft mit Filialen unabhängiger zu machen. Gerade den vielen kleineren und mittleren Händlern helfen die großen Verkaufsplattformen relativ schnell und einfach neue Kundschaft zu gewinnen. In der Coronakrise, in der viele Läden geschlossen waren, mutierten die Onlineplattformen teils für manche Händler zur einzigen starken Umsatzquelle. Der Zustrom zu den Marktplätzen ist entsprechend groß.

Die Marktplätze wie z.B. von Otto allerdings sehen sich grundsätzlich nicht in der Pflicht sich stärker für den Schutz von Daten zu engagieren. Es gebe schließlich die Verpflichtung der Händler sich an den Datenschutz zu halten. So weigerten sie sich, wie in der Datenschutz-Grundverordnung (DSGVO) vorgesehen Benachrichtigung der betroffenen Kunden vorzunehmen. In ihrer Ansicht wurden sie von einem Sprecher des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen bestärkt, der meinte, dass das Fehlen eines Auftragsvertrags mit den Plattformanbietern diese von ihrer Verantwortlichkeit befreit.

Eine der betroffenen Kundinnen ist Christa Reise-Zunft aus Stuttgart. Sie hatte im März 2021 mehrere Kissenfüllungen auf Kaufland.de bestellt. Durch das Datenleck waren ihre Post- und Mailadresse sowie Rechnung und Bestelldaten im Netz: „Ich denke, die Daten sind geschützt. Die Plattformen müssen die Leute doch darüber benachrichtigen.“

Diese Ansicht wird vom Datenschutzexperten Thilo Weichert geteilt: „Art. 33 und 34 DSGVO verpflichten Verantwortliche zur unverzüglichen Benachrichtigung der zuständigen Aufsichtsbehörde und der Betroffenen über ein Datenleck, bei dem ein hohes Risiko für die Betroffenen besteht. Diese Pflicht haben bei einer gemeinsamen Verantwortlichkeit alle Stellen, so wie dies hier der Fall ist. Otto&Co. waren und sind insofern in der Pflicht. Für die Online-Kunden besteht der zutreffende Eindruck es hier nicht nur mit dem einzelnen Händler, sondern auch mit der Marktplattform zu tun zu haben. Auch wenn formal kein Vertrag mit dem Dienstleister besteht, so besteht ein Vertrag mit dem Händler, für dessen Dienstleister die Plattform nach Datenschutzrecht eine Mitverantwortung trägt.“ Anders als oft die Händler seien die Plattformbetreiber auch in der Lage auf Sicherheitsverstöße schnell und adäquat zu reagieren.

Die zuständigen Landesdatenschutzbeauftragten haben den Fall um das Datenleck untersucht. Dass die betroffenen Kunden seit Monaten nicht informiert worden sind, ist auch für Stefan Brink, den Landesdatenschutzbeauftragten von Baden-Württemberg, ein „schwerwiegender und skandalöser Vorgang“. Der Schweizer IT-Sicherheitsexperte Mark Ruef hat die Daten analysiert und überprüft, ob sie möglicherweise schon

im Darknet gehandelt worden sind: „Die Daten sind sehr konkret, es sind auch Zahlungsinformationen dabei. Damit könnte man Phishing-Mails füllen oder Identitätsdiebstahl begehen.“ Ob die betroffenen Datensätze tatsächlich im Darknet gehandelt worden seien, lasse sich final allerdings nicht mehr klären, weil das Datenleck drei Jahre lang bestand (Beuth/Gnirke, IT-Experte entdeckt Informationen von 700.000 Käufern, www.spiegel.de 01.07.2021; Gräfe, Nutzerdaten jahrelang online, www.tagesschau.de 12.01.2022).

Bundesweit

Datenschutzkonferenz: Gegen die Auskunfteispeicherung von Positivdaten

Wirtschaftsauskunfteien wie die Schufa oder Crif Bürgel sammeln die Vertragsdaten von mutmaßlich Millionen deutscher Mobilfunkkunden, ohne dass dafür eine Einwilligung vorliegt. Bei den Daten handele es sich um seit 2018 gesammelte Angaben zum Vertragsabschluss, zur Dauer des Vertrages und einem Vertragswechsel, Verbindungsdaten sind nicht betroffen. Die deutschen Datenschützer vertreten die Ansicht, dass Auskunfteien solche Daten nur verarbeiten dürfen, wenn eine ausdrückliche Einwilligung der Betroffenen vorliegt. Lediglich die Auskunftei Infoscore Consumer Data erklärte, sie speichere solche Daten nicht. Crif Bürgel betonte, man nutze Handyvertragsdaten nicht zur Bonitätsbewertung.

Am 22.09.2021 hatte die Datenschutzkonferenz (DSK) der Aufsichtsbehörden der Bundesländer in einem Beschluss bekräftigt, dass Auskunfteien sogenannte Positivdaten, die nicht zur Erfassung etwa von Zahlungsverzügen bei Krediten notwendig sind, nicht unter Berufung auf die in der Europäischen Datenschutz-Grundverordnung (DSGVO) vorgesehenen Ausnahmen speichern dürfen. Sie begründet dies damit, dass durch diese Praxis „große Datenmengen über übliche Alltagsvorgänge im Wirtschaftsleben erhoben und verarbeitet wurden“ – völlig ohne Anlass. Vielmehr verlangt die DSK, dass es „einer wirksamen Einwilligung der betroffenen Person unter Beachtung der hohen Anforderungen an die Freiwilligkeit bedarf“. Einem Sprecher des Landesbeauftragten für Datenschutz von Nordrhein-Westfalen gemäß wollen die Unternehmen die Einholung einer Einwilligung vermeiden und berufen sich auf ihr „berechtigtes Interesse“.

Gemäß dem Branchenverband „Die Wirtschaftsauskunfteien“ würde ohne die Daten, z.B. zum Mobilvertrag, eine Kreditwürdigkeitsprüfung „unnötig erschwert“. Insbesondere „finanzschwächere Menschen“ würden von der Verarbeitung profitieren, etwa Migranten, junge Konsumenten und häufig auch Seniorinnen. Der Chef des Verbraucherzentrale Bundesverbands (vzbv) Klaus Müller meinte dagegen, hier werde der Bock zum Gärtner gemacht. Das Argument, finanzschwächeren Menschen etwas Gutes zu tun, würde „instrumentalisiert“, es würden ganz andere Interessen verfolgt. Er hat die Sorge, dass die Auskunfteien die Menschen bewerten und diese keine Verträge mehr bekommen, weil sie beispielsweise den Vertrag wechseln oder oft Rabatte abstauben: „Das ist ein falscher Weg – und es hat nichts mit dem Mantel der Barmherzigkeit zu tun.“

Es wird unterschieden zwischen Negativ- und Positivdaten. Negativdaten sind solche, die anfallen, wenn ein Verbraucher z.B. einen Kredit nicht bezahlt. Für diese Speicherung kann es wichtige Gründe geben. Bei Positivdaten, so Müller, sei dies aber grundlegend anders. Positivdaten sind Informationen, dass z.B. jemand überhaupt ein Konto bei einem Mobilfunkunternehmen hat, auch wenn er seine Rechnungen pünktlich bezahlt. Was genau mit diesen Daten passiert, ist selbst den Landesdatenschützern nicht im Detail bekannt, man sei vom eher intransparenten Verhalten der Auskunfteien „enttäuscht“.

Die Daten werden u.a. für das sogenannte Scoring benutzt. Dabei wird aus verschiedenen Daten ein Wert berechnet, der Rückschlüsse auf die Bonität von Verbrauchern zulassen soll. Die dafür verwendeten Algorithmen halten die Auskunfteien geheim. Das Scoring wird von Verbraucherschützern schon lange kritisiert. Müller: „Damit werde ich gläserner als ich es jemals gewesen bin. Das ist eine Entwicklung, die wir Verbraucherschützer falsch finden, die wir ablehnen und von der Datenschutz-Grundverordnung in dieser Form, unserer Meinung nach, nicht abgedeckt ist.“

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit Alexander Roßnagel erklärte, dass nun die Auskunfteien gefordert seien „ihre Datenerhebungs- und Verarbeitungsprozesse zu ändern“. vzbv-Vorstand Müller fordert, dass „dieser wertvolle Beschluss“ der Datenschutzkonferenz nun auch durchgesetzt werden muss. Die Daten müssten gelöscht werden. Immerhin sei die DSGVO kein zahnloser Tiger. Offenbar ist zu der Frage schon eine gerichtliche Klage anhängig.

Auch auf europäischer Ebene wird über das Scoring gestritten. Im Hinblick auf die laufende Reform der EU-Richtlinie für Verbraucherkredite fordert der EU-Datenschutzbeauftragte Wojciech Wiewiórowski genau festzulegen, welche Datenkategorien zur Bewertung der Kreditwürdigkeit verwendet werden dürfen. Wiewiórowski empfiehlt überdies, dass alle in der DSGVO als besonders sensibel eingestuften Daten nicht zum Scoring verwendet werden sollten.

Unterdessen befasst sich derzeit auch der Europäische Gerichtshof (EuGH) mit der Frage, ob und wie die Verarbeitung von Scoring-Daten und deren Weitergabe mit der DSGVO vereinbar ist. Laut der DSGVO dürfen Personen „nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen“ werden. Ob die Ausnahme für „Abschluss oder die Erfüllung eines Vertrags“ für das Scoring gilt, haben die EuGH-Richter nun zu klären. Sonst bliebe als Arbeitsgrundlage der Auskunfteien § 31 des Bundesdatenschutzgesetzes (BDSG), bei dem deutsche Richter Zweifel haben, dass er europarechtskonform ist. Auch diese Frage soll nun der EuGH beantworten (DSK, Beschluss v. 22.09.2021, Verarbeitung von Positivdaten von Privatpersonen aus Verträgen über Mobilfunkdienste und Dauerhandelskonten durch Auskunfteien; Wischmeyer, Einwilligung nicht erteilt, SZ 01.12.2021, 18; Briegleb, Scoring: Schufa & Co. sammeln Handyvertragsdaten ohne Einwilligung, www.heise.de 01.12.2021, Kurzlink: https://heise.de/-6281597).

Bundesweit

Klarna – Finanzmonster ohne Verbrauchertransparenz

Gegen das milliardenschwere Fintech-Unternehmen Klarna sind in der Berliner Datenschutzbehörde mehr Beschwerden aufgelaufen als gegen alle anderen Banken und Versicherungen zusammen. Der schwedische Bezahlspezialist bündelt mit seiner Super-App, also einer mehrere Apps oder Funktionen vereinigenden Anwendung, Shopping und Girokonto. Nutzer können nach einer Registrierung in der App überall einkaufen ohne sich bei jedem Online-Shop neu anmelden zu müssen. Auch Preissenkungen sollen über die App zu erkennen sein.

Wenn ein Shop noch nicht den Klarna-Bezahldienst integriert hat, generiert Klarna für die Zahlung eine Einmalkreditkarte. Die Daten aus den Stöber-, Einkaufs- und Bezahlvorgängen nutzt Klarna, um individuelle Einkaufsvorlieben auszumachen und Einkaufsvorschläge zu unterbreiten. Die Auslieferung und das Paket-Tracking sind ebenfalls in die App integriert, womit auch verschiedene Ortsdaten gesammelt werden können. Klarna will so erreichen, dass Kunden nur noch über die Klarna-Super-App einkaufen gehen. Vorbild sind die chinesischen Super-Apps Wechat und Alipay. Paypal kündigte kürzlich an ebenfalls eine Super-App bauen zu wollen, doch die Umsetzung lässt noch auf sich warten.

Klarna gehört zu den Deacorns der Startup-Szene: Investoren bewerten das 2009 gegründete Unternehmen mit 45 Mrd. US-Dollar. Obwohl Klarna wie ein veritabler Bankenkonzern wirkt, agiert das Unternehmen gegenüber Kunden eher im Startup-Modus. Abteilungsleiter Daniel Holzapfel von der zuständigen Berliner Datenschutzbehörde (BlnBDI) berichtet, dass Ende 2021 rund hundert Beschwerden gegen das schwedische Fintech-Unternehmen vorliegen.

Bekannt wurde das Fintech mit der für viele Online-Shops angebotenen Option „Zahlen auf Rechnung“. Kunden wählen diese Option oft in der Annahme, dass dadurch keine sensiblen Finanzdaten bei einem Online-Bezahldienst entstehen. Tatsächlich setzen sie dabei aber eine umfangreiche Bonitätsprüfung in Gang, für die erheblich mehr Daten generiert werden, als für eine einfache Online-Bezahlung. Bei Klarna können Kunden über ihr Konto u.a. Kredite aufnehmen, um die Online-Käufe zu bezahlen. Die Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin) mahnt Käufer bei solchen Angeboten ausdrücklich im Rahmen ihrer finanziellen Möglichkeiten zu bleiben und die effektiven Jahreszinsen zu vergleichen. Klarna betreibt auf sozialen Plattformen wie Instagram Influencer-Kampagnen, die für die Flexibilität der Ratenzahlung werben, wo Kunden ihre Raten auch aussetzen können. Sara Elisa Kettner, Verhaltensforscherin von der Berliner Denkfabrik Conpolicy, weist darauf hin, dass dies aber, ohne sofort erkennbar zu sein, mit sehr hohen Zinsen erkauft wird. Problematisch seien auch an junge Verbraucher auf TikTok adressierte Klarna-Challenges – etwa im Sinne von „Ich habe bei Klarna 2.000 Euro Schulden. wer kann das überbieten?“ – möglicherweise mit einem späten Erwachen.

Mit der Super-App fließen nicht nur Transaktionsdaten, sondern auch Bestelldaten und Kaufhistorien bei Klarna zu Nutzerprofilen zusammen. Die Hälfte der Beschwerden beim BlnBDI bezieht sich auf den Anspruch der Nutzer auf Auskunft beziehungsweise Löschung ihrer Daten. Sie monieren, dass Klarna zeitweise viele weitere Daten erfragte, bevor Nutzer ihren Anspruch letztendlich durchsetzen konnten. Inzwischen soll sich das geändert haben. Weitere Beschwerden beziehen sich auf Identitätsdiebstahl: Die Kunden fanden keinen direkten Ansprechpartner und konnten nur auf automatisierte Formularantworten reagieren. Ein E-Bike-Vermieter, der die Zahlungen über Klarna abwickelte, verifizierte offenbar nicht die angegebenen Adressdaten. Auch sogenannte Komfortfunktionen irritieren: So soll die E-Mail-Adresse genügen, um alle weiteren Daten ausfüllen zu können.

Die Berliner Datenschützer versuchten die Beschwerden zunächst im direkten Kontakt mit der Berliner Zweigstelle des Unternehmens zu klären. Ihr einziger deutscher Ansprechpartner hat das Unternehmen verlassen. Einen neuen gibt es nicht. Dies führt nun dazu, dass sich auch die zuständige schwedische Datenschutzaufsichtsbehörde intensiver mit Klarna befasst.

- Erklärung erklärt nichts

Klarnas Datenschutzerklärung, die eigentlich alle wesentlichen Fragen klären soll, steht mit Stand 29.10.2021 auf rechtlich tönernen Füßen. Die DSGVO verlangt von den Unternehmen ihre Datenschutzbestimmungen in klarer und einfacher Sprache zu formulieren. Ziel ist es die Nutzer und Verbraucherinnen so zu informieren, dass sie verstehen, was mit ihren Daten geschieht. Klarna hat für seine App eine Datenschutzerklärung verfasst, die ausgedruckt in einer PDF-Datei rund 60 Seiten umfasst. Dazu Elisa Kettner: „Bei 14.000 Wörtern ist mit einer Lesezeit von 1,5 Stunden zu rechnen.“ Mit Klarnas Datenschutzerklärung könnten Verbraucher im Grunde also keine informierte Einwilligung erteilen, wie sie die DSGVO im Sinn hat.

Nach Ansicht des Datenschutzexperten Thilo Weichert verstößt die Datenschutzerklärung im Web gegen sämtliche DSGVO-Transparenzpflichten (Art. 12 ff. DSGVO): „Die aufgeführten ‚Informationen‘ tun nichts anderes als alle vorstellbaren Zwecke zu benennen und dann den Gesetzeswortlaut wiederzugeben.“ Wo Klarna konkreter werden müsste, bleibe das Unternehmen schmallippig: „Wenn irgendwelche Stellen beteiligt werden, so werden diese nicht präzise benannt, sondern nur als Kategorie, eventuell ergänzt durch eine Liste sämtlicher wichtigen Stellen, die in dieser Kategorie tätig sind.“ Das sei keine Information in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“, wie sie Artikel 12 DSGVO verlange. Die Beliebigkeit der Information bestehe „durchgängig“. Google mit seinem Recaptcha-Dienst und anderen möglichen Diensten wird erwähnt, aber nicht erklärt. Dass Übermittlungen in Drittländer erfolgen, wird zwar mitgeteilt, aber nicht genau wohin und auf welcher konkreten rechtlichen Grundlage.

Die komplette Datenschutzerklärung, sei eine „grandiose Nebelmaschine, aus der die konkreten Datenverarbeitungen weder nachvollzogen, geschweige denn

auf ihre Plausibilität hin überprüft werden könnten." Dass damit unzulässige Verarbeitungsprozesse verschleiert werden sollen, „schimmert an vielen Ecken durch". So wird die „ausdrückliche Einwilligung" zur Verarbeitung von sensitiven Daten im Kleingedruckten eingeholt.

Eine Sprecherin von Klarna wies in Reaktion auf die Vorwürfe darauf hin, dass das Unternehmen „in Ergänzung zu unserer Vollversion" auch „eine ausführliche, transparente und leicht zugängliche Datenschutzerklärung in einer einfachen und klaren Sprache zur Verfügung" stellen würde. Kunden würden bei jeder einzelnen Datenschutzanfrage unterstützt. Klarna habe „niemals die Absicht als ´Gate Keeper` zu agieren". Weichert kann darin keine Hilfe sehen, sondern nur eine beschönigende Manipulation, wenn als Zwecke angegeben wird: „um Ihr Einkaufserlebnis zu verbessern" oder „damit wir unsere Produkte auf Sie zuschneiden, Ihnen Unterstützung anbieten können".

- Wer ist verantwortlich?

Klarnas Super-App agiert als digitaler Türsteher, der darüber entscheidet, welcher Händler in die heiligen Hallen der App darf – und wer nicht. Klarna steht zwischen dem Kunden und den Händlern, weshalb bereits der Handelsverband Deutschland (HDE) vor einer Monopolisierung des Kundenzugangs warnt. Klarna trifft keine Aussagen darüber, wie mit den Daten aus dem Geschäftsprozess zwischen Händler und Bezahldienstleister umgegangen wird. Diese sogenannte gemeinsame Verantwortlichkeit erwähnt Klarna in seiner überaus wortreichen Datenschutzerklärung aber an keiner Stelle. Zudem, so Weichert: „Da ist einmal von der Klarna-Group die Rede. Was aber wer in der Group macht, ist absolut unklar. Die ganze Datenschutzerklärung ist ein dicker Buchstabensalat, in dem nichts drinnen steht." Der Berliner Datenschützer Daniel Holzapfel hält es daher für sinnvoll das Thema Datenschutzerklärung 2022 auf die Agenda zu setzen (Schulzki-Haddouti, Klarna: Super-App mit Super-Datenschutzproblemen, www.golem.de 24.12.2021).

Baden-Württemberg/Berlin

Betroffeneninformation über Funkzellenabfragen

Als erstes Bundesland hat Berlin seit Mitte September 2021 ein Funkzellenabfragen-Transparenz-System (FTS) im Echtbetrieb und informiert die Bürger darüber, ob ihre Handynummer bei einer Funkzellenabfrage der Polizei erfasst wurde. Das baden-württembergische Justizministerium will dieses FTS nach dem Berliner Modell auch einführen und hat bereits Planungen und Vorbereitungen eingeleitet.

Das FTS informiert alle, die zum Zeitpunkt der Funkzellenabfrage im System angemeldet waren, per SMS. Die Anmeldung dafür ist freiwillig, kostenlos und das Interesse unter den Berlinern ist laut Mitteilung des Justizministeriums hoch: Seit 2018 gab es 18.000 Registrierungen. Zum September waren 3.500 Nummern angemeldet. Die Benachrichtigung findet jeweils erst nach Abschluss des Ermittlungsverfahrens statt, um die Ermittlungen nicht zu gefährden.

Das Innenministerium in Stuttgart erklärte in Beantwortung einer parlamentarischen AfD-Anfrage: „Das Justizministerium begleitet die Erfahrungen der Berliner Kollegen und steht mit diesen in engem Austausch. Gegen die Einführung eines FTS bestehen aus strafprozessualer Sicht keine Bedenken." Aus einer Mitteilung des Bundesamtes für Justiz (Stand: 12.02.2021) geht hervor, dass die Strafverfolgungsbehörden in Baden-Württemberg im Jahr 2019 insgesamt 1.600 zuvor gerichtlich angeordnete Funkzellenabfragen in insgesamt 1.453 Ermittlungsverfahren durchgeführt haben. Bei jeder Funkzellenabfrage werden alle Mobilfunknummern, die sich zum Abfragezeitraum in der Funkzelle befinden, erfasst.

Beim Berliner FTS ist zunächst eine freiwillige und kostenlose Anmeldung für den Dienst erforderlich. Angemeldete Handybesitzer erhalten dann nach Abschluss eines Ermittlungsverfahrens per SMS einen Bescheid, wenn ihre Mobilfunknummer in einer Abfrage erfasst wurde. Anschließend sollen die Daten gelöscht werden. Funkzellenabfragen sind in der Strafprozessordnung geregelt. Sie müssen demnach von der Staatsanwaltschaft beantragt und von einem Richter genehmigt werden (Wittenhorst, Baden-Württemberg: Handybesitzer sollen über Funkzellenabfrage informiert werden, www.heise.de 20.11.2021. Kurzlink: https://heise.de/-6273105).

Berlin

Tests mit automatischer Parkraumüberwachung

Das Berliner Bezirksamt Mitte testete im Berliner Grunewald Anfang Dezember 2021 erstmals, wie sich parkende Fahrzeuge mit Hilfe eines ScanCar genannten Autos automatisch überwachen und erfassen lassen. Bei dem Modellprojekt wird eine Technik zur digitalen Parkraumüberwachung in ausgewählten Bezirken erprobt. Ziel ist die „mobile Prüfung digitaler Parkberechtigungen (‚virtuelle Parkscheine / Vignetten')" durch Scanfahrzeuge. Dafür werden Parkstände vorab erfasst. Der Berliner Senat verspricht sich davon, den Parkdruck, den Parksuchverkehr und das Falschparken zu reduzieren. Gleichzeitig soll auf diese Weise weniger Personal benötigt werden, da die Straßen nicht mehr von Menschen nach Parksündern abgesucht werden müssten.

Eingesetzt wird in Berlin dafür die Technik ScanGenius des niederländischen Herstellers Arvoo. Mehrere Kameras in einem Dachaufbau scannen rundum die Umgebung und können Nummernschilder erfassen. Diese werden mit der GPS-Ortung kombiniert. Die Parkraumbewirtschaftung erledigt die niederländische Firma Egis, die ihr System beispielsweise seit 2017 in Amsterdam betreibt.

Wer sein oder ihr Auto an einem bewirtschafteten Parkplatz abstellt, gibt auf dem Smartphone oder am stationären Automaten das Kfz-Kennzeichen ein. Diese Kennzeichen werden mit den vom Scancar erfassten und in einer Datenbank gespeicherten abgeglichen. Wenn das System feststellt, dass ein Fahrzeug nicht in der Park-Datenbank enthalten ist, wird das Kfz-Kennzeichen an die Bußgeldstelle weitergeleitet. Auf diese Weise sollen pro Stunde 2.000

parkende Autos kontrolliert werden können, während eine Ordnungshüterin auf bis zu 300 Autos am Tag kommt. Bisher allerdings gibt es für die Kennzeichenerfassung zur Parkraumüberwachung keine Rechtsgrundlage. Der am 30.11.2021 unterzeichnete Berliner Koalitionsvertrag von SPD, Grünen und FDP enthält den Passus: „Wir wollen eine Öffnung für digitale Anwendungen wie digitale Parkraumkontrolle." Laut Bezirksbürgermeisterin Monika Hermann lassen sich die Kameras des Scancars so einstellen, dass sie ausschließlich die Kennzeichen erfassen (Wilkens, Berlin testet digitale Parkraumüberwachung mit Scancars, www.heise.de 07.12.2021, Kurzlink: https://heise.de/-6288527).

Berlin

Hunderttausende Corona-Schnelltest-Daten im Netz

Durch eine ungeschützte Online-Schnittstelle, die mehrere Berliner Corona-Testanbieter gemeinsam nutzten, waren persönliche Daten von mehreren hunderttausend Personen im Internet offen abrufbar. Von dem Datenleck betroffen waren personenbezogene Informationen wie Name, Anschrift, Telefonnummer, E-Mail-Adresse und das Ergebnis der Getesteten. In einigen Fällen waren auch die Nummern von Personalausweis oder Pass der Betroffenen dabei.

Die Sicherheitslücke bei den Zentren, die sich unter dem Namen „Schnelltest Berlin" zusammengeschlossen hatten, entdeckte das IT-Kollektiv „Zerforschung". Diesem zufolge prüfte der Server über https://corona-api.de/ nicht, ob ein abgerufenes Testergebnis das der zugehörigen Person ist. Anhand der Personenliste schätzen die IT-Sicherheitsexperten, dass fast 700.000 Testergebnisse von rund 400.000 Kunden abrufbar gewesen seien. Die Berliner Landesdatenschutzbehörde ging zunächst von über 200.000 Betroffenen aus.

Im Quellcode entdeckten die Experten zudem die Endpunkte, über die Mitarbeiter einen neuen Test im System anlegen und das Testergebnis speichern können. Der Server überprüfte auch hier keine Berechtigung. Die Hacker machten die Probe aufs Exempel und generierten einen PCR-Test mit negativem Ergebnis für den 177-jährigen Robert Koch. Das ausgegebene Zertifikat enthielt sogar einen „BärCODE" als vermeintliches Sicherheitsmerkmal, der bei einem Scan mit der zugehörigen Prüf-App auch als gültig erkannt wurde.

Die Firma WeCare Services betreibt die IT-Infrastruktur für die Anbieter von „Schnelltest Berlin". Gemäß dem Unternehmen wurden die Sicherheitslücken umgehend geschlossen. Die Betroffenen würden kurzfristig informiert. Neben 15 Testzentren in der Hauptstadt, die unter dem Verbundnamen auftreten, gehören zu dem Zusammenschluss auch mobile Corona-Bike-Testpunkte, auf die oft Event-Veranstalter und Clubs setzen. Die Zerforscher hatten zuvor bei einigen anderen Testanbietern ebenfalls Schwachstellen aufgedeckt (Krempl, Corona-Schnelltests: Daten von Hunderttausenden im Netz, Zertifikate fälschbar, www.heise.de 10.11.2021, Kurzlink: https://heise.de/-6263796).

Niedersachsen

Datenpanne bei Geodatenbehörde

Wegen einer Datenpanne muss Niedersachsens Landesamt für Geoinformation und Landvermessung (LGLN) rund 25.000 möglicherweise betroffene Online-Kunden informieren. Eine Behördensprecherin teilte am 11.01.2022 mit, dass Namen, Anschriften, Mailadressen und eventuell auch Telefonnummern von Kunden, die digitale Produkte des LGLN online bezogen haben, entwendet wurden und ins Netz gelangt sind. Die Behörde warnt die Kunden vor möglichen Phishing-Mails, in denen sie zur Eingabe von schutzwürdigen Informationen aufgefordert werden könnten. Vorsorglich werden Online-Kunden der letzten zwei Jahre informiert. Das LGLN habe sämtliche Webdienste gleicher Bauart zunächst offline genommen, um sie einer tieferen Analyse von internen und externen Experten zu unterziehen. Auch das niedersächsische Landeskriminalamt (LKA) und die Landesdatenschutzbeauftragte seien informiert worden. Eine Reihe von Diensten wie zum Beispiel „Bodenrichtwerte online" funktionierten weiterhin. Wer zum Beispiel für einen Grundstückskauf Daten und Karten benötige, solle sich per Mail an das zuständige Katasteramt wenden. Die entsprechenden Informationen würden dann zur Verfügung gestellt (Datenpanne in Landesamt in Niedersachsen: Möglicherweise 25.000 Kunden betroffen, www.heise.de 11.01.2022, Kurzlink: https://heise.de/-6322844).

Nordrhein-Westfalen

Bettina Gayk neue Chefin des LDI NRW

Der Landtag von Nordrhein-Westfalen hat am 19.05.2021 einstimmig Bettina Gayk zur neuen Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes Nordrhein-Westfalen (LDI NRW) gewählt. Sie folgt damit Helga Block, die das Amt seit 2015 innehatte und im Sommer 2020 in den gesetzlichen Ruhestand eingetreten ist. Herbert Reul beglückwünschte die Leitende Ministerialrätin aus seinem Haus zur Wahl: „Bettina Gayk bringt eine Spitzen-Erfahrung mit; sie weiß wirklich, was Datenschutz bedeutet und kennt das Thema seit vielen Jahren. In meinem Haus wird sie für ihre Kompetenz und ihre Freundlichkeit sehr geschätzt. Für uns ein Verlust, für den Datenschutz in Nordrhein-Westfalen ein Riesengewinn."

Gayk war seit 2012 im nordrhein-westfälischen Innenministerium tätig; als Referatsleiterin verantwortete sie zuletzt den Brand-, Katastrophen- und Zivilschutz und war stellvertretende Abteilungsleiterin. Ihre Karriere begann Gayk im Jahr 1991. Als Beamtin des Landes Nordrhein-Westfalen absolvierte die studierte Juristin zunächst Stationen bei der Bezirksregierung Düsseldorf, der Stadt Velbert und in Hilden. Von 2001 bis 2012 arbeitete sie bereits in der Datenschutzaufsichtsbehörde des Landes, die damals von den Landesdatenschutzbeauftragten Bettina Sokol und Ulrich Lepper geleitet wurden, als Referatsleiterin und Pressesprecherin.

Gayk benannte als eines ihrer primären Aufgaben eine bessere Präsenz ihrer Behörde im Internet: „Die Öffentlichkeitsarbeit liegt mir sehr am Herzen. Nur wenn wir die Menschen erreichen, um deren Daten es schließlich geht, können wir diese Grundrechte effektiv schützen. In meiner neuen Funktion möchte ich zum Beispiel mein eigenes Werk von damals, das immer noch online ist, den aktuellen Ansprüchen anpassen. Schließlich will ich die Bürgerinnen und Bürger möglichst nutzerfreundlich und einfach informieren" (Bettina Gayk neue Landesbeauftragte, www.im.nrw 19.05.2021).

Rheinland-Pfalz

Luca-App-Daten illegal für strafrechtliche Ermittlungen genutzt

Obwohl Daten der Luca-App für die Strafverfolgung tabu sein sollten, hat das Polizeipräsidium Mainz bei Ermittlungen zu einem Sturz mit Todesfolge auf Daten der Luca-App zugegriffen. Mittels einer Datenabfrage wurden Besucher einer Gaststätte in der Mainzer Innenstadt ausfindig gemacht, um diese als mögliche Zeugen des Vorfalls zu gewinnen, der sich am 29.11.2021 ereignet hatte. Ein Besucher war nach dem Verlassen der Gaststätte offenbar so gestürzt, dass er einige Tage später aufgrund seiner Verletzungen starb.

Die Polizei suchte am 13.12.2021 auch mit einer Pressemitteilung nach Zeugen. Eine verantwortliche Mitarbeiterin der Gaststätte gab an, dass Beamtinnen und Beamte der Mainzer Kriminalpolizei nach dem Vorfall auch aktiv nach Daten aus der Luca-App gefragt haben, offenbar, um mit an diesem Abend Anwesenden sprechen zu können. Später hatte sie dann via Luca-App eine Bitte des Gesundheitsamts Mainz um Datenfreigabe bezüglich der am 29.11.2021 anwesenden Gäste erhalten. Dieser habe sie stattgegeben.

Einer der Gäste an jenem Abend berichtete, er sei dann am 20.12.2021 von der Polizei in Mainz kontaktiert worden, mit dem Hinweis, dass seine Kontaktdaten via Luca-App gewonnen worden sind. Die Nutzung von Daten der Luca-App, die in vielen Gaststätten und Restaurants zur Corona-Kontaktverfolgung eingesetzt wird, ist unter anderem laut Infektionsschutzgesetz (IfSG) aus datenschutzrechtlichen Gründen für die Strafverfolgung unzulässig. Auch die Landesregierung Rheinland-Pfalz wirbt auf ihrer Website ausdrücklich damit, dass die anhand der Luca-App gewonnenen Daten nicht für die Strafverfolgung verwendet würden. Auf corona.rlp.de heißt es: „Die zur Kontaktnachverfolgung erhobenen Daten dürfen nach § 28a Abs. 4 des Infektionsschutzgesetzes sowie nach § 1 Abs. 8 der Corona-Bekämpfungsverordnung Rheinland-Pfalz nicht zu anderen Zwecken verwendet werden."

Die Staatsanwaltschaft Mainz bestätigte die Datenabfrage mit Hilfe der Luca-App in Zusammenhang mit dem Fall. Insgesamt seien so 21 potentielle Zeugen ausfindig gemacht und angerufen worden. Dies sei mit der entsprechenden Polizeibehörde abgestimmt gewesen und aufgrund einer fehlerhaften Bewertung des Infektionsschutzgesetzes erfolgt. Tatsächlich gebe es für die Datenabfrage „keine hinreichende rechtliche Grundlage". Man habe bereits den behördlichen Datenschutzbeauftragten informiert. Auch der Landesdatenschutzbeauftragte werde unterrichtet.

Mitarbeiterinnen und Mitarbeiter der Staatsanwaltschaft würden hinsichtlich der Rechtslage sensibilisiert: „Die Staatsanwaltschaft Mainz drückt ihr Bedauern gegenüber den insoweit vom unzulässigen Zugriff auf die Daten Betroffenen aus und bittet darum diesen Zugriff zu entschuldigen. Es wird sichergestellt, dass die entsprechenden Daten nicht weiter genutzt werden." Die Staatsanwaltschaft habe eine Prüfung veranlasst, inwiefern in weiteren Ermittlungsverfahren auf Daten der Luca-App zurückgegriffen worden sei. Bisher sei kein weiterer Fall bekannt.

Der Datenschutzbeauftragte von Rheinland-Pfalz, Dieter Kugelmann, sah mit dem Zugriff auf Kontaktinformationen aus dem System hinter der Luca-App durch Strafverfolger „das Vertrauen der Bürger in die Rechtmäßigkeit staatlichen Handelns" erschüttert. Das Vorgehen sei „gerade in Zeiten einer die Gesellschaft als Ganzes herausfordernden Pandemie das völlig falsche Signal". Der Experte für Polizeirecht hat „umgehend aufsichtsrechtliche Verfahren" eingeleitet. Dabei sollen insbesondere die Umstände geklärt werden, die ungeachtet der eindeutigen Rechtslage zu der datenschutzrechtlich unzulässigen Abfrage und Nutzung der ausschließlich zu Infektionsschutzzwecken erfassten Kontaktdaten geführt haben. Besorgniserregend ist für Kugelmann vor allem, „dass sowohl Staatsanwaltschaft als auch Gesundheitsamt die bereits vor einiger Zeit geänderte Rechtslage im Infektionsschutzgesetz und damit zusammenhängende datenschutzrechtliche Bestimmungen offensichtlich nicht kannten oder sich darüber hinweggesetzt haben". Die Sanktionsmöglichkeiten der Kontrolleure sind gegenüber staatlichen Stellen aber deutlich eingeschränkter als bei privaten Unternehmen, wo die Datenschutz-Grundverordnung greift.

Nach dem Vorfall riefen rheinland-pfälzische Politiker von Grünen und FDP dazu auf, das digitale Tool von Mobiltelefonen zu löschen. Der netzpolitische Sprecher der Grünen im Landtag, Alexander Salomon, meinte: „Was die Warnung und die Nachverfolgung angeht, ist die Luca-App mausetot."

Die Macher der Luca-App kritisierten den Missbrauch scharf. Die Mainzer Gesundheitsbehörde habe auf Druck beziehungsweise Bitten der Polizei wohl „einen Infektionsfall simuliert", um die an sich geschützten Daten entschlüsseln zu können. Der Rapper Smudo als Mitentwickler des Systems nannte Aufrufe, die nach den Berichten über den polizeilichen Datenzugriff laut wurden, die Luca-App zu deinstallieren, „verantwortungslos". Luca helfe gegenwärtig jeden Tag, Infektionsketten zu unterbrechen. Experten halten die Anwendung dagegen für unwirksam, da die Arbeitslast in den Gesundheitsämtern in den mehrfachen Corona-Wellen zu hoch sei. Die dort Beschäftigten kämen gar nicht dazu die gelieferten Kontaktdaten nachzuverfolgen (Mainzer Polizei nutzte Daten der Luca-App, www.tagesschau.de 07.01.2022; Grüne: Luca-App „mausetot", SZ 10.01.2022, 7; Krempl, Zugriff auf Luca-Daten: Datenschützer sieht Rechtsstaatlichkeit untergraben, www.heise.de 12.01.2022, Kurzlink: https://heise.de/-6324593).

Schleswig-Holstein

Sensible Ausländerbehörden-Daten bei eBay

Michael S. erwarb bei eBay im Auftrag seines Unternehmens bei zwei Auktionen insgesamt 13 PCs vom Typ Fujitsu D756 SFF vom Verkäufer onkellaepi2020. Die Rechner sollten eigentlich ohne Festplatte geliefert werden, doch in einem steckte eine drin. Der PC mit einem gelben Punkt an der Gerätefront, wie alle Rechner aus der Lieferung, zeigte beim Aufruf von Windows 7 einen Desktop-Hintergrund der Hansestadt Lübeck.

Immer wieder finden sich Behörden-PCs mitsamt Festplatte bei eBay. Die an die c´t-Redaktion weitergebene Festplatte wurde daraufhin von dem dort bestehenden IT-Labor analysiert. Der PC mit dem Windows-Namen „LS46-WS-1091" war anscheinend im Ausländeramt der Hansestadt eingesetzt worden. Er enthielt Daten aus der Zeit vom 20.01.2016 bis zum 29.06.2021 mit 31 nicht gelöschten Nutzerkonten. 18 Mitarbeiter waren so namentlich als auch mit ihrer Funktion in der Behörde zu identifizieren. Darunter waren Mitarbeiterinnen wie Anja B. (anonymisierte Namensangaben), die nur wenige Monate im Ausländeramt ihr Referendariat ableistete, oder Berta C., die offenbar im Jahre 2019 zehn Monate lang für den Telefonservice des Amts zuständig war. Ein langjähriger Mitarbeiter Claus D. war als Sachbearbeiter „Aufenthaltsbeendigung" tätig, Dieter E. wohl im Gebäudemanagement und möglicherweise auch im Personalrat der Behörde.

Die Daten auf der Festplatte geben Hinweise auf die Arbeitsweise der Ausländerbehörde. So scheint es einen zentralen Scanner zu geben, über den eingehende Dokumente erfasst und dann per E-Mail an die zuständigen Sachbearbeiter weitergeleitet werden. Auch Faxe an die Behörde werden augenscheinlich per E-Mail verteilt. Aus diesen Dokumenten entstehen dann komplette Vorgangsakten, die sich Mitarbeiter anscheinend in größeren Mengen vom zentralen Server herunterladen können. 48 komplette Akten unter anderem zu Visa-Anträgen, die im Download-Verzeichnis des Users Starketh zu finden waren, legen dies nahe.

Die vom System als „Gesamtakte" bezeichneten PDF-Dateien wurden zwischen 12. und 21.10.2020 auf dem Arbeitsplatzrechner gespeichert. Jede Akte enthält Personendaten aller an dem Visa-Antrag Beteiligten, also auch Verdienst- und Vermögensnachweise deutscher Bürger, wie sie bei der Einladung von Freunden und Verwandten aus dem nicht visabefreiten Ausland üblicherweise gefordert werden. Die E-Mail-zentrierte Arbeitsweise der Behörde führte zum größten Datenfund auf der Festplatte: Mehr als 33.400 E-Mails mit hochbrisanten Inhalten zu Asyl- als auch zu Ausweisungsverfahren waren mühelos ohne Einsatz forensischer Werkzeuge auf dem Datenträger auszumachen.

Zu allen möglichen Vorgängen in einem Ausländeramt waren passende Daten zu finden: Einbürgerungen, Namensänderungen, Grenzübertrittsbescheinigungen, Wiedereinreisesperren, Fahndungsausschreibungen, Abschiebungsanordnungen, Meldeakten. In den E-Mails und ihren Anhängen auf der Festplatte fanden sich solche Vorgänge nebst zugehörigen Betroffenendaten.

Dabei handelte es sich zum Teil um höchst sensible Daten nach Art. 9 DS-GVO mit Angaben zu Religion, sexueller Ausrichtung oder ethnischer Herkunft. Diese Informationen sind besonders streng zu schützen.

Schuld an diesem über Jahre angehäuften Datengrab war vor allem der Einsatz von Microsoft Outlook als E-Mail-Client. Zwar nutzt die Hansestadt Lübeck einen zentralen Server auf dem alle E-Mails gespeichert werden. Doch in der Standardkonfiguration legt Microsoft Outlook für jeden Nutzer versteckte sogenannte OST-Dateien an. In diesen hinterlegt Outlook jede geöffnete oder versendete Nachricht. Selbst vermeintlich gelöschte Nachrichten finden sich in den OST-Dateien wieder.

Zweck des lokalen Zwischenspeichers ist Reduzierung der Serverlast und Verringerung des Netzwerkverkehrs. Erkauft wird das mit sich daraus zwangsläufig ergebenden Datenschutzproblemen. Zwar lässt sich MS-Outlook so konfigurieren, dass keine lokalen Zwischenspeicher entstehen. Vielen Admins ist das aber nicht bekannt – oder sie scheuen diese Option, weil der Zugriff auf E-Mails dann merklich langsamer werden kann. Wer im Behördenumfeld und beim Umgang mit sensiblen Personendaten unbedingt MS-Outlook nutzen will, muss zumindest dafür sorgen, dass die Daten auf der Festplatte verschlüsselt hinterlegt werden. Andernfalls kann jeder mit physischem Zugriff auf den PC die Daten leicht lesen oder gar extrahieren. Verschlüsselung kostet ein bisschen Performance.

Nach Auskunft der Datenschutzbeauftragten für Schleswig-Holstein, Marit Hansen, schreibt das Land vor, dass Datenträger mit sensiblen Daten wie Festplatten vor der Verwertung ausgemusterter PCs aus dem Rechner entfernt und anschließend vernichtet werden müssen. In der Hansestadt Lübeck scheint das so geregelt zu sein, dass Mitarbeiter der Stadt die Festplatten ausbauen, die PCs dann mit einem gelben Punkt versehen und den Rechner anschließend an einen Verwerter übergeben. Im Falle der gefundenen und von Journalisten ausgewerteten Festplatte wurde da offenbar geschlampt. Nach Aussage des Verwerters trug der via eBay verkaufte PC zwar einen gelben Punkt, ob in dem Rechner dann aber auch wirklich keine Platte mehr war, hätte er nicht überprüft. Die mit der Hansestadt Lübeck getroffene Verwertungsvereinbarung sehe nicht vor, dass er jeden einzelnen PC noch einmal aufschrauben und überprüfen müsse.

Die Hansestadt Lübeck gab sich nach Mitteilung des Vorfalls einsilbig. Bürgermeister Jan Lindenau meinte, aufgrund der laufenden Ermittlungen könnten leider keine Angaben gemacht werden. Man habe den Vorfall an die Landesdatenschutzbehörde gemeldet und Anzeige erstattet. Gleichzeitig forderte er die Redaktion auf die Festplatte mit den Daten des Ausländeramts Lübeck zu übergeben. Diese teilte dem Bürgermeister mit, dass die Festplatte bis auf Weiteres in sicherer Verwahrung bleibe. Die Datenschutzbehörde aus Schleswig-Holstein kündigte an sich die Sache sehr genau anzusehen (Schnurer, 33.000 hochsensible Mails aus dem Ausländeramt Lübeck bei eBay verkauft, www.heise.de 28.01.2022, Kurzlink: https://heise.de/-6335260).

Datenschutznachrichten aus dem Ausland

Weltweit

Google scannt Drive-Cloud-Inhalte

Google hat in einem Blogbeitrag Mitte Dezember 2021 eine neue Richtlinie für den Cloud-Speicherdienst Drive angekündigt, wonach er künftig den Zugriff auf Dateien einschränken wird, die gegen die Unternehmensrichtlinien und die Nutzungsbedingungen verstoßen. Diese betreffen eine breite Palette strafbarer und schädlicher Inhalte. Sie reicht von Cybercrime-Tatbeständen über den Schutz des Urheberrechts bis hin zu Darstellungen sexuellen Kindesmissbrauchs.

Der Internetkonzern will von sich aus Schritte unternehmen, um einschlägige, auf seiner Plattform gehostete Dateien zu identifizieren, die mit Upload-Filtern flächendeckend gescannt werden. Schlagen die dafür eingesetzten Algorithmen an, werden die entsprechenden Dateien dem Nutzer angezeigt und automatisch für Dritte gesperrt. Sie können also nicht mehr mit anderen Personen geteilt werden. Der Zugriff auf bereits verbreitete Inhalte wird allen außer dem Uploader entzogen.

Als Begründung führt der Konzern Folgendes aus: „Dies wird dazu beitragen, dass die Eigentümer von Google Drive-Elementen vollständig über den Status ihrer Inhalte informiert sind.“ So werde sichergestellt, „dass die Nutzer vor missbräuchlichen Inhalten geschützt sind“. Zudem will sich Google selbst gegen den Missbrauch der eigenen Dienste besser absichern.

Die „Richtlinien zur Verwendung von Google-Produkten“, die nun stärker durchgesetzt werden sollen, untersagen u.a. „gefährliche und illegale Aktivitäten“, „Belästigung, Mobbing und Drohungen“ sowie „Hassrede“. Nicht geduldet werden zudem Identitätsdiebstahl und Falschdarstellungen, Malware, Phishing, Spam und „nicht einvernehmliche, freizügige“ Bilder wie Nacktaufnahmen sowie Pornografie allgemein. Ausnahme: „Gestattet ist Nacktheit zu pädagogischen, dokumentarischen, wissenschaftlichen oder künstlerischen Zwecken.“ Aufgeführt werden auf der langen Liste ferner etwa „irreführende Inhalte“, nicht autorisierte Bilder von Minderjährigen, Blut und drastische Gewaltdarstellung sowie Propaganda gewalttätiger Organisationen und Bewegungen. Auch urheberrechtlich geschützte Inhalte dürfen nicht ohne Genehmigung geteilt oder Links auf Webseiten verbreitet werden, auf denen solches Material illegal heruntergeladen werden kann. Wiederholte Verstöße führen hier „zur Kündigung Ihres Kontos“.

Google begründet den Vorstoß: „Wir müssen Missbräuche eindämmen, die unsere Fähigkeit bedrohen diese Dienste bereitzustellen.“ Alle Nutzer werden gebeten sich an die Vorgaben zu halten: „Nachdem wir über einen möglichen Verstoß gegen die Richtlinien informiert wurden, können wir den Inhalt überprüfen und Maßnahmen ergreifen, einschließlich der Einschränkung des Zugriffs auf den Inhalt, der Entfernung des Inhalts und der Beschränkung oder Beendigung des Zugriffs eines Nutzers auf Google-Produkte.“ Wie das Unternehmen zwischen rechtmäßigen Dateien und Inhalten, die gegen die Vorschriften verstoßen, im Detail unterscheiden will, bleibt offen. Um sicherzustellen, dass die mehrfach erwähnten Ausnahmen für legitime Zwecke greifen, müssten eigentlich menschliche Begutachter über die Upload-Filter wachen und die letzte Entscheidung treffen.

Der Konzern äußerte sich hierzu nicht. Er verwies nur allgemein darauf, dass man bei dem Cloud-Service ständig daran arbeite „die Sicherheit unserer Nutzer und der Gesellschaft zu schützen und dabei stets die Privatsphäre zu wahren“. Bei Google Mail würden Inhalte seit Langem auf Spam sowie Phishing- und Malware-Angriffe gescannt. Nun sei es wichtig diese Praxis auch für Google Drive zu übernehmen, damit der Dienst „für alle Nutzer so sicher wie möglich bleibt“. Google analysierte Mails lange auch, um Nutzern gezielte personenbezogene Werbung anzuzeigen. 2017 stellte das Unternehmen diese Praxis ein, nachdem unter anderem Datenschützer Druck gemacht hatten. 2018 wurde bekannt, dass Drittentwickler weiterhin in die Gmail-Postfächer schauen und Millionen Mails lesen können.

In der EU können Google, Facebook, Microsoft und andere Diensteanbieter, die etwa bei Chats, Video-Calls und E-Mails keine Ende-zu-Ende-Verschlüsselung einsetzen, die privaten Nachrichten ihrer Nutzer in der EU seit Kurzem wieder freiwillig rechtmäßig nach sexuellen Missbrauchsdarstellungen von Kindern scannen. Das EU-Parlament hatte dazu im Juli per Eilverordnung Ausnahmen von der Anwendung einiger Bestimmungen der E-Privacy-Richtlinie zum Datenschutz in der elektronischen Kommunikation eingeführt. Die EU-Kommission arbeitet mit Unterstützung des Ministerrats an einem Folgegesetz, um diese umstrittene „Chatkontrolle“ für alle einschlägigen Dienstleister verpflichtend zu machen (Krempl, Google scannt Cloud-Dateien nach rechtswidrigen und schädlichen Inhalten, www.heise.de 18.12.2021, Kurzlink: https://heise.de/-6298682).

Weltweit

Strafverfolger bestücken „Have I Been Pwned“

Die Nationale Kriminalbehörde Großbritanniens NCA (National Crime Agency) hat eine Datenbank mit fast 600 Mio. sichergestellten Passwörtern gemäß dem Projektverantwortlichen Troy Hunt an das Projekt Have I Been Pwned weitergegeben; über 225 Mio. waren dort noch nicht in der Datenbank. Wer den Dienst nutzt, kann also nun auch herausfinden, ob eigene Zugangsdaten in diesem neuen Datensatz enthalten sind. Der lag demnach auf einem kompromittierten Cloud-Server und sei keiner Plattform zuzuordnen gewesen.

Have I Been Pwned hat darüber hinaus jetzt auch eine bereits angekündigte Schnittstelle, über die Strafverfolgungsbehörden solche Datensätze schneller an das Projekt geben können.

Für diese Erweiterung hat Hunt mit der US-Bundespolizei FBI zusammengearbeitet. Dafür hat er das System in eine Open-Source-Software umgewandelt und den Quellcode verfügbar gemacht. Hunt hatte im Frühjahr 2021 damit begonnen. Den Aufwand hatte er unterschätzt und war dann von der .NET Foundation unterstützt worden, einer von Microsoft unterstützten Non-Profit-Organisation. Dank der neuen Kooperation kann das Projekt nun viel schneller aktualisiert werden, wenn ein Leak bekannt wird und erbeutete Datensätze öffentlich werden.

Hunt hatte seinen Passwort-Prüfdienst Ende 2013 eröffnet, inspiriert durch einen immensen Hack bei Adobe. Seitdem ist er eine immer beliebter gewordene Anlaufstelle für Internetnutzer, die erfahren wollen, ob ihre Zugangsdaten im Zuge eines Hacks kompromittiert wurden. Dazu bindet Hunt verfügbar gewordene Datenbanken ein. Interessierte können dann prüfen, ob es für ihre E-Mail-Adresse darin einen Treffer gibt. Hunt stellt zusätzlich eine API für eine automatisierte Abfrage bereit. 2019 hatte Hunt angekündigt den Dienst verkaufen zu wollen, dann aber grundsätzlichen Zweifel an dem Plan bekommen. Aus dem Verkauf wurde nichts. Have I Been Pwned soll auf absehbare Zeit hin unabhängig bleiben (Holland, Have I Been Pwned: 225 Millionen neue Passwörter von britischer Polizeibehörde, www.heise.de 21.12.2021, Kurzlink: https://heise.de/-6301963).

Weltweit

Meta schließt einige Spionageaccounts aus

Der Facebook-Konzern Meta teilte am 16.12.2021 mit, dass rund 50.000 Nutzerinnen und Nutzer ins Visier von Überwachungsfirmen geraten sind, die sie ausspionieren wollten. Die Betroffenen seien hierüber unterrichtet worden. Meta, zu dem auch Instagram und WhatsApp gehören, habe mehrere Unternehmen von seinen Plattformen verbannt. Dafür seien rund 1.500 Scheinkonten entfernt worden, über die Informationen über Nutzer in mehr als 100 Ländern gesammelt worden seien.

Die Überwachungsfirmen stammen demnach aus Israel, Indien und Nordmazedonien. Zu den von Meta genannten Unternehmen gehören Black Cube sowie Bluehawk CI aus Israel, BellTroX, eine indische Cyber-Söldnerfirma, die im vergangenen Jahr von Reuters und dem Internet-Watchdog Citizen Lab enttarnt wurde, und ein europäisches Unternehmen namens Cytrox. Auch eine nicht näher identifizierte Gruppe aus China habe versucht Nutzer auszuspionieren. Black Cube ist für ihren Einsatz im Auftrag des ehemaligen Hollywood-Produzenten und Sexualstraftäters Harvey Weinstein bekannt. Als Basis für das Vorgehen gegen die Firmen verweist Meta darauf, dass diese gegen Nutzungsbedingungen verstoßen hätten.

Die betroffenen Nutzer leben Facebook zufolge unter anderem in den USA, Neuseeland, Mexiko, Hongkong und Polen. Sie seien zunächst beobachtet und auskundschaftet worden. Danach hätten die Firmen häufig versucht über fingierte Accounts mit ihnen Kontakt aufzunehmen, um Überwachungssoftware auf ihre Geräte zu bringen.

WhatsApp verklagte bereits vor einiger Zeit den israelischen Überwachungssoftware-Spezialisten NSO, weil dessen „Pegasus“-Software gegen Nutzer des Chatdienstes eingesetzt worden sei (Rund 50.000 Nutzer im Visier von Überwachungsfirmen, www.horizont.net 17.12.2021; Weniger Spione auf Facebook, SZ 18./19.12.2021, 24).

EU

EDSB beanstandet Corona-Test-Webseite des EU-Parlaments

Der Europäische Datenschutzbeauftragte (EDSB) Wojciech Wiewiórowski monierte am 05.01.2022, dass das Europäische Parlament auf seiner Corona-Test-Seite rechtswidrig u.a. Google Analytics eingebunden hat. Er verlangte, dass das Parlament seine Covid-19-Test-Webseite innerhalb eines Monats nachbessert und die Privatsphäre der Nutzer besser absichert. Er rügte auf Beschwerde mehrerer Abgeordneter und der Bürgerrechtsorganisation noyb, dass das Parlament auf seiner Seite für das Testzentrum gegen das Datenschutzrecht verstoßen hat.

Während der Corona-Pandemie setzt das Parlament auf ein Testcenter des Anbieters EcoCare, für das sich die Mitglieder der Institution im Intranet registrieren können. Beim Zugriff auf die Webseite entdeckten Volksvertreter, dass diese anfangs mehr als 150 Anfragen von Drittanbietern verschickte. Darunter waren auch die US-Unternehmen Google und Stripe. Wiewiórowski hob in seiner Entscheidung hervor, dass der Einsatz von Google Analytics und des Zahlungsanbieters Stripe nicht mit dem Schrems II-Urteil des Europäischen Gerichtshofs (EuGH) zum Transfer personenbezogener Daten zwischen der EU und den USA vereinbar ist. Die Luxemburger Richter hatten dort erneut festgestellt, dass US-Sicherheitsgesetze eine Massenüberwachung ermöglichen und der Datenschutzstandard in den Vereinigten Staaten daher nicht dem in der EU entspricht.

Die Ansage Wiewiórowskis ist eine der ersten Entscheidungen zur Umsetzung von „Schrems II“ in der Praxis. Sie könnte für zahlreiche weitere einschlägige Fälle wegweisend sein, die zurzeit Gerichte und Regulierungsbehörden behandeln. Zuvor hatte z.B. das Verwaltungsgericht Wiesbaden einer Hochschule auf Basis des EuGH-Grundsatzurteils untersagt auf ihrer Homepage den „Cookiebot“ einzubinden und Daten so in die USA zu übermitteln (vgl. in diesem Heft S. 60).

Die erste Beschwerde beim EDSB hatte die Grüne Alexandra Geese im Namen weiterer Abgeordneter wie Patrick Breyer (Piratenpartei) eingereicht. noyb untermauerte dieses Vorgehen vor einem Jahr mit einer weiteren Eingabe. Die Beschwerdeführer beanstandeten auch, dass die Cookie-Banner der Webseite unklar und irreführend seien: Die Betreiber hätten darin nicht alle platzierten Browser-Dateien aufgelistet, zudem habe es Unterschiede zwischen unterschiedlichen Sprachversionen gegeben. Folglich sei es den Nutzern nicht möglich gewesen, eine gültige Zustimmung zu erteilen. Das Parlament entfernte daraufhin alle Cookies.

Der EDSB bestätigte ferner die Auffassung der Beschwerdeführer, dass die Datenschutzinformationen des Testzen-

trums nicht klar und verständlich gewesen seien. Damit habe das Parlament gegen die Transparenzpflicht verstoßen. Zudem habe das Gremium Auskunftsersuchen nicht korrekt beantwortet.

Die Aufsichtsbehörde erteilte dem Parlament einen Verweis für die verschiedenen Verstöße gegen eine spezielle, für die EU-Institutionen geltende Datenschutzverordnung. Dazu kommen eine Verwarnung und eine Unterlassungsanordnung mit einer Frist von einem Monat. Im Gegensatz zu den nationalen Datenschutzbehörden kann Wiewiórowski nur unter bestimmten Umständen eine Geldstrafe verhängen, die in diesem Fall nicht erfüllt waren. Die hier nicht greifende Datenschutz-Grundverordnung bietet mehr Spielraum für Sanktionen (Krempl, EU-Datenschützer verwarnt Parlament wegen Datentransfer an Google und Stripe, www.heise.de 11.01.2022, Kurzlink: https://heise.de/-6323169).

EU

EDSA erläutert Auskunftsanspruch nach Art. 15 DSGVO

Der Europäische Datenschutzausschuss (EDSA bzw. EDPB – European Data Protection Board), hat am 15.01.2022 beschlossene Leitlinien zum Recht auf Auskunft nach Art. 15 DSGVO veröffentlicht (Guidelines 1/2022). Der EDSA ist das wichtigste Gremium der europäischen Datenschutzaufsichtsbehörden. Es besteht aus Vertretern der Datenschutzbehörden aller EU-Mitgliedsstaaten und dem Europäischen Datenschutzbeauftragten, der für den Datenschutz bei den Organen und Einrichtungen der EU zuständig ist.

In dem 60 Seiten starken Dokument setzen sich die Datenschutzaufsichtsbehörden mit zahlreichen, in der Praxis teilweise äußerst umstrittenen Fragen auseinander. Der EDSA geht außer auf die Form der Übermittlung der jeweiligen Auskunft an den Betroffenen auf die formellen Anforderungen an Auskunftsersuchen ein und macht Vorgaben in Bezug auf die Identifikation des Betroffenen. Er beantwortet die Frage, wann ein Auskunftsersuchen als offenkundig unbegründet oder exzessiv angesehen und damit abgelehnt werden kann. Die Unbegründetheit von Auskunftsersuchen wird in der Praxis recht häufig zur Abwehr von Auskunftsersuchen vorgebracht und war bereits häufiger Gegenstand von gerichtlichen Entscheidungen, insbesondere auch im Arbeitsrecht.

Der EDSA befürwortet eine weite Auslegung des Auskunftsanspruchs und legt die Möglichkeiten des Verantwortlichen, das Auskunftsersuchen zurückzuweisen, eng aus. Der Text versteht sich als Entwurf, zu dem der EDSA im Rahmen eines öffentlichen Konsultationsverfahrens insbesondere Verbände und Interessenvertreter zur Einreichung von Stellungnahmen aufruft. Bei Leitlinien und Stellungnahmen der Datenschutzaufsichtsbehörden handelt es sich stets um Empfehlungen, denen keine rechtliche Bindungswirkung zukommt. Auch wenn diese keine Rechtssicherheit bringen, so geben sie Hinweise auf das Verständnis der Aufsichtsbehörden und sind ein bedeutender Impuls für die Debatte und wichtiger Orientierungspunkt für den Umgang mit Auskunftsersuchen (Hessel, EU-Datenschutzaufsichtsbehörden befürworten weites Auskunftsrecht, www.heise.de 28.01.2022, Kurzlink: https://heise.de/-6342280; https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf).

EU

Datenschutzbeauftragter gegen Targeting bei Polit-Werbung

Der Europäische Datenschutzbeauftragte Wojciech Wiewiórowski fordert in einer am 20.01.2022 veröffentlichten Stellungnahme, dass der Gesetzentwurf der EU-Kommission für mehr Transparenz bei politischer Werbung nachgeschärft wird. Er empfiehlt, Microtargeting bei Wahlwerbung vollständig zu verbieten. Gemäß dem Kommissionsvorschlag sollen Anbieter politischer Online-Anzeigen nur besonders sensible Daten nicht mehr für politische Zwecke nutzen. Sie dürften also Informationen etwa über die politische Einstellung, sexuelle Orientierung, Religion, Gesundheit oder ethnische Herkunft nicht mehr ohne Zustimmung der Betroffenen verwenden, um einschlägige Werbung auf eine Person per Microtargeting und dem damit verknüpften Erstellen von Psychogrammen zuzuschneiden.

Wiewiórowski will erreichen, dass für politische Botschaften von Datensammlern wahrgenommene Präferenzen oder Interessen der Adressaten überhaupt nicht eingesetzt werden dürfen. Das Online-Verhalten der Betroffenen müsse in diesem Fall komplett außen vor bleiben. Der Datenschutzbeauftragte spricht sich zudem dafür aus, dass weitere Einschränkungen bei personenbezogenen Daten eingeführt werden sollten, die zum Zweck der politischen Werbung verarbeitet werden dürfen. Dies müsse vor allem für Fälle gelten, in denen eine solche Wähleransprache den Einsatz von Targeting-Techniken beinhaltet: „Politische Kommunikation ist für Bürger, politische Parteien und Kandidaten unerlässlich, um voll am demokratischen Leben teilnehmen zu können. Um unsere Demokratie zu bewahren, brauchen wir auch strenge Regeln, um Desinformation, Wählermanipulation und Eingriffe in unsere Wahlen zu bekämpfen." Die EU müsse daher mehr unternehmen, um die mit Targeting-Verfahren verknüpften Risiken anzugehen. Parallel macht sich das EU-Parlament dafür stark über den geplanten Digital Services Act (DSA) allgemein „spionierende Werbung" anhand sensibler persönlicher Daten zu untersagen (Krempl, Politische Werbung: EU-Datenschützer fordert komplettes Targeting-Verbot, www.heise.de 21.01.2022, Kurzlink: https://heise.de/-6335147).

EU

Polizeivernetzung, vor allem mit Gesichtsbildaustausch, wird vorangetrieben

Der Prümer Vertrag, der bislang den Austausch etwa von Gen- und Fingerabdruckdaten in der EU regelt (DANA 1/2021, 16), soll erweitert werden. Einbezogen werden dürfen laut dem am 08.12.2021 veröffentlichten Vorschlag der EU-Kommission für einen Kodex

für die polizeiliche Zusammenarbeit künftig auch Fahndungsfotos oder biometrische Lichtbilder in polizeilichen Datenbanken, die eine automatisierte Gesichtserkennung unterstützen.

Die Initiative findet sich im Entwurf der Kommission für eine Verordnung „über den automatisierten Datenaustausch für die polizeiliche Zusammenarbeit", der Teil des vorgelegten Gesetzespakets ist. Der 2005 begründete Prüm-Rahmen soll um Gesichtsbilder von Verdächtigen und verurteilten Straftätern sowie um Strafregisterdaten ergänzt werden.

Ferner wird dem Plan zufolge auf EU-Ebene ein zentraler Router eingerichtet, an den die nationalen Polizei-Datenbanken angeschlossen werden können. Damit sollen sich die bisher benötigten „zahlreichen Verbindungen zwischen den einzelnen nationalen" IT-Systemen im Strafverfolgungsbereich erübrigen. Für Europol ist die Befugnis vorgesehen die Mitgliedstaaten effizienter zu unterstützen. Die Den Haager Polizeibehörde soll Daten aus Drittländern mit den Datenbanken der EU-Länder abgleichen dürfen, um Straftäter zu identifizieren, die jenseits der Grenzen der Gemeinschaft bekannt sind.

Gemäß der Kommission soll Europol zu einem integralen Bestandteil des Prüm-Vertrags werden. Die Mitgliedstaaten würden auch in die Lage versetzt die dort gespeicherten biometrischen Daten von Nicht-EU-Ländern zu überprüfen. Insgesamt solle der Ansatz gewährleisten, „dass keine Lücken in den von Nicht-EU-Ländern erhaltenen Daten über Kriminalität und Terrorismus entstehen".

Derzeit erfolgt der Austausch von Gesichtsbildern und polizeilichen Aufzeichnungen zwischen den Mitgliedstaaten. Gemäß der Initiative fehlt ein effizientes EU-weites Abgleichverfahren, das die Möglichkeiten zur Identifizierung von Tätern erheblich erhöht. Dabei könnten auch verschiedene Identitäten oder mehrere Straftaten aufgedeckt werden, die von derselben Person in anderen EU-Ländern begangen wurden.

Künftig soll ein Foto einer unbekannten Person, das etwa eine Überwachungskamera an einem Tatort aufgenommen hat, mit einer Datenbank abgeglichen werden können, die Gesichtsbilder bekannter Personen enthält. Die mithilfe biometrischer Gesichtserkennung ausgegebene Trefferliste werde dann von einer menschlichen Fachkraft im anfragenden Mitgliedstaat überprüft. Die Suche könne nur im Zusammenhang mit einer bestimmten strafrechtlichen Ermittlung und nach Begehung einer Straftat durchgeführt werden.

Weiter heißt es: „Ein Abgleich von Gesichtsbildern mit der Allgemeinbevölkerung findet nicht statt". Auch der Einsatz von Künstlicher Intelligenz sei nicht vorgesehen. Die Suche erfolge rückwirkend. Eine Live-Gesichtserkennung oder biometrische Fernidentifizierung großer Personengruppen in öffentlichen Räumen sei damit nicht möglich. Es werde auch keine zentrale Datenbank für Fahndungsfotos errichtet. Zudem gälten die „robusten" Grundsätze der Datenschutzrichtlinie für Polizei und Justiz weiter.

Die Kommission hält einige der Prüm-Vorschriften über die technischen Spezifikationen von Abfragen, Sicherheitsmaßnahmen und Kommunikation für „veraltet". Wissenschaft und Technik hätten sich auf diesem Feld in den vergangenen zehn Jahren erheblich weiterentwickelt. Unterschiedliche nationale Vorschriften und Verfahren für das weitere Vorgehen bei einem „Treffer" könnten ferner „zu erheblichen Verzögerungen beim Informationsaustausch führen".

Die Kommission hat ihre Initiative langfristig vorbereitet, indem sie etwa beim Beratungs- und Dienstleistungshaus Deloitte eine Machbarkeitsstudie für ein erweitertes Prüm-Verfahren in Auftrag gab. Die Experten rieten dazu den Vertrag auf „neue Datenkategorien" auszudehnen. Der Ministerrat setzte parallel „Fokusgruppen" zum europaweiten Austausch von Gesichtsbildern ein, die aus Brüssel eine halbe Million Euro erhielten. Aus Deutschland war das Bundeskriminalamt (BKA) beteiligt. Die Verordnung muss noch das EU-Parlament und den Rat passieren.

Kritiker bezeichneten das Vorhaben schon früh als hochproblematisch. Mitgliedsländer könnten das System etwa nutzen, um gezielt politische Gegner zu verfolgen. Die Bürgerrechtsorganisation European Digital Rights (EDRi) warnt, durch die geplante zusätzliche Automatisierung würden „wichtige verfahrenstechnische und gerichtliche Schutzmaßnahmen" ausdrücklich aufgehoben. Prüm II berge auch die Gefahr zu verstärkter Diskriminierung, da die Polizei bestimmte ethnische und marginalisierte Bevölkerungsgruppen öfters kontrolliere. Jede Gesichtsdatenbank erhöhe das Risiko einer biometrischen Massenüberwachung. Oft würden in solchen Registern viele Unschuldige gespeichert.

Mit einer Richtlinie will die Kommission zudem gewährleisten, dass Polizeibeamten in einem Mitgliedstaat unter denselben Bedingungen der gleiche Zugang zu Informationen gewährt wird wie ihren Kollegen vor Ort. Es sollen rund um die Uhr besetzte zentrale Kontaktstellen eingerichtet werden, um den Austausch über die Secure Information Exchange Network Application (SIENA) von Europol zu beschleunigen. Dazu kommt der Entwurf für eine Ratsempfehlung für erweiterte operative Einsätze etwa in Grenzgebieten zwischen EU-Ländern. Damit sollen etwa gemeinsame Polizeipatrouillen erleichtert und dazu „sichere Kommunikationssysteme" eingeführt werden (Krempl, Fahndung: EU-Kommission drängt auf EU-weiten Abgleich von Gesichtsbildern, www.heise.de 08.12.2021, Kurzlink: https://heise.de/-6289814).

EU/Irland

Bürgerrechtsorganisation: Irischer Datenschutz ist ungenügend

Die Bürgerrechtsorganisation Irish Council for Civil Liberties (ICCL) hat am 29.11.2021 eine formelle Beschwerde gegen die EU-Kommission bei der Europäischen Bürgerbeauftragten Emily O'Reilly eingereicht, in der der Kommission vorgeworfen wird, nicht gegen Irlands Versäumnisse bei der Anwendung der Datenschutz-Grundverordnung (DS-GVO) vorzugehen. 98% der großen, von der irischen Data Protection Commission (DPC) betreuten Fälle von EU-weiter Bedeutung sind demnach noch immer ungelöst, obwohl das Gesetz schon dreieinhalb Jahre gelte.

Die Behäbigkeit der irischen Datenschutzbehörde habe zur Folge, dass die Durchsetzung der EU-Rechtsvorschriften gegen große US-Internetkonzerne wie Google, Facebook, Microsoft und Apple „gelähmt wird". Die Kommission sei als Hüterin der EU-Verträge dafür verantwortlich, dass die Mitgliedstaaten das EU-Recht einhalten. Sie sei so auch befugt Mitgliedstaaten andernfalls vor dem Europäischen Gerichtshof zu verklagen. Die DPC ist die federführende Aufsichtsbehörde im Rahmen der DSGVO für große Technologieunternehmen, die ihren europäischen Hauptsitz in Irland haben. Andere Kontrolleure in der EU können dann nicht direkt eingreifen. Die ICCL kritisiert, dass Irlands Versäumnis so die gesamte Gemeinschaft gefährdet.

Laut der Beschwerde tut die Kommission generell zu wenig, um die Einhaltung der DSGVO ordnungsgemäß zu überwachen. Sie habe bei den Mitgliedsstaaten nicht einmal ausreichende Informationen erhoben, um ein Urteil darüber fällen zu können. Einschlägige Statistiken, die der Europäische Datenschutzausschuss (EDSA) als Gremium der Kontrollbehörden an die Brüsseler Exekutivinstanz weitergeleitet hat, seien unzureichend. Es bleibe unklar, in wie vielen Fällen die einzelnen Datenschutzbeauftragten federführend seien, wie oft die Behörden von ihren Ermittlungs- oder Sanktionsbefugnissen Gebrauch gemacht hätten und wie viele Tage von einer Beschwerde bis zu einer endgültigen Entscheidung vergingen.

Die DPC gilt ihren Kritikern bereits seit Längerem als Flaschenhals bei der DSGVO-Durchsetzung. Auch das EU-Parlament forderte jüngst die Kommission auf, deswegen ein Vertragsverletzungsverfahren gegen Irland einzuleiten. Johnny Ryan vom ICCL hatte vor Kurzem auf strukturelle Probleme bei der unterfinanzierten Behörde aufmerksam gemacht. Sie habe zu wenige Online-Ermittler und nutze fürs Beschwerdemanagement noch immer Lotus Notes. Dies sei so, als ob man die Gehaltsabrechnung für viele Mitarbeiter mit einem Rechenschieber bewältigen wolle (Krempl, Mangelnde DSGVO-Durchsetzung: Beschwerde gegen EU-Kommission eingeleitet, www.heise.de 30.11.2021, Kurzlink: https://heise.de/-6280112).

Österreich

Datenschutzbehörde: Google Analytics verstößt gegen EuGH-Vorgaben

Die Nutzung von Google Analytics auf Webseiten in der EU ist nach Ansicht der österreichischen Datenschutzbehörde (DSB) mit der Datenschutz-Grundverordnung (DSGVO) nicht vereinbar. Die DSB sieht vor allem die allgemeinen Grundsätze der Datenübermittlung gemäß Art. 44 DSGVO verletzt, da mit dem Statistikprogramm persönliche Nutzerinformationen an die Google-Konzernzentrale in den USA weitergegeben werden. Mit dem Teilbescheid reagiert die DSB auf eine Musterbeschwerde, die der vom Juristen und Aktivisten Max Schrems gegründete Datenschutzverein noyb im August 2020 erhoben hatte. Die Eingabe bezog sich zunächst auf einen österreichischen Verlag, der Google Analytics eingebunden hat. Eine weitergehende Beschwerde gegen Google selbst wies die DSB ab.

Die DSB meint in ihrem Beschluss, der Webseitenbetreiber habe mit dem Statistikwerkzeug personenbezogene Daten des Beschwerdeführers an Google übermittelt. Dazu zählten einzigartige Nutzer-Identifikationsnummern, die IP-Adresse und Browserparameter. Googles Standardvertragsklauseln böten kein „angemessenes Schutzniveau", um die „Überwachungs- und Zugriffsmöglichkeiten durch US-Nachrichtendienste" nach dem Foreign Intelligence Surveillance Act (FISA) zu beseitigen. Hintergrund der Entscheidung ist das „Schrems II"-Urteil des Europäischen Gerichtshofs (EuGH) vom Sommer 2020, mit dem dieser den transatlantischen „Privacy Shield" und damit eine der wichtigsten Grundlagen für den Transfer von Kundendaten in die USA für ungültig erklärte (DANA 3/2020, 199 ff.). Die Luxemburger Richter stellten dabei fest, dass US-Gesetze wie FISA oder der Cloud Act eine Massenüberwachung durch Sicherheitsbehörden ermöglichen und der Datenschutzstandard in den Vereinigten Staaten nicht dem in der EU entspricht.

Google hatte zuvor eingewandt, im Rahmen der Standarddatenschutzklauseln „technische und organisatorische Maßnahmen" (TOMs) ergriffen zu haben wie Verschlüsselungstechniken, Zäune um Datenzentren und die Überprüfung von Behördenanfragen (vgl. DANA 4/2021, 250 f.). Die DSB bewertete diese Maßnahmen aber als weitgehend nutzlos gegenüber den Ansprüchen von Geheimdiensten wie der NSA oder der Polizeibehörde FBI. Die EU-Kommission bemühte sich in Folge der EuGH-Entscheidung, die Standardvertragsklauseln als alternatives Instrument für Datenübermittlungen an die EuGH-Rechtsprechung anzupassen und veröffentlichte die neue Version Anfang Juni 2021. Google implementierte diese überarbeiteten Vorgaben im September 2021 für die eigenen Cloud-Dienste. Das Unternehmen kündigte dabei auch an, stärker auf Verschlüsselung setzen zu wollen.

Schrems hält solche Vorkehrungen nicht für ausreichend. Er kritisierte: „Anstatt ihre Dienste technisch so anzupassen, dass sie mit der DSGVO konform sind, haben US-Unternehmen versucht einfach ein paar Texte in ihre Datenschutzrichtlinien einzufügen und den EuGH zu ignorieren. Viele EU-Unternehmen sind diesem Beispiel gefolgt anstatt auf legale Dienste zu wechseln." Die Quintessenz der DSB-Entscheidung ist für den noyb-Gründer: „EU-Unternehmen können keine US-Cloud-Dienste mehr nutzen."

Betroffen sieht Schrems die Betreiber sehr vieler Webseiten in der EU, da Google Analytics noch immer das am weitesten verbreitete Statistikprogramm sei. Obwohl es viele Alternativen gebe, die in Europa gehostet werden oder auf eigenen Servern laufen können, verließen sich noch zu viele Administratoren auf den US-Konzern. Insgesamt hat noyb 101 vergleichbare Beschwerden in fast allen EU-Staaten eingereicht. Schrems geht daher davon aus, dass ähnliche Entscheidungen nun schrittweise auch dort fallen werden. Nicht zufrieden ist noyb damit, dass die DSB die Beschwerde gegen Google als Datenempfänger in den USA zurückgewiesen hat. Man prüfe, gegen diesen Teil der Entscheidung vorzugehen. Zugleich habe die Aufsichtsbehörde aber erklärt, dass das Verfahren gegen Google mit Blick auf mögliche Verstöße gegen andere Artikel der DSGVO weiterlaufe. Dazu

werde es wohl noch eine eigene Entscheidung geben (Krempl, Österreichs Datenschutzbehörde: Google Analytics verstößt gegen die DSGVO, www.heise.de 13.01.2022, Kurzlink: https://heise.de/-6326506).

Frankreich

CNIL geht gegen Clearview AI vor

Die französische Datenschutzbehörde CNIL (Commission Nationale de l'Informatique et des Libertés) verlangt in einem Beschluss von Ende November 2021 von der auf biometrische Gesichtserkennung spezialisierten US-Firma Clearview AI „die Sammlung und Nutzung von Daten von Personen einzustellen, die sich auf französischem Hoheitsgebiet befinden". Sie sieht für diese umstrittene Praxis des Fotoabgleichs keine Rechtsgrundlage. Clearview soll es betroffenen französischen Bürgern zudem erleichtern ihre Rechte auszuüben. Anträgen auf Löschung persönlicher Daten sei stattzugeben.

Die CNIL setzte der New Yorker Firma eine Frist von zwei Monaten, um die in der Mahnung formulierten Anordnungen zu befolgen und dies gegenüber der Aufsichtsbehörde nachzuweisen. Andernfalls drohten Sanktionen wie „insbesondere eine Geldstrafe". Die Kontrolleure hatten seit Mai 2020 Beschwerden einzelner Personen über die von Clearview entwickelte Gesichtserkennungssoftware erhalten (vgl. DANA 1/2020, 68, 2/2020, 125). Ein Jahr später wandte sich auch die Bürgerrechtsorganisation Privacy International deswegen an sie. Bei den Untersuchungen arbeitete die CNIL nach eigenen Angaben mit europäischen Kollegen zusammen: Da das Unternehmen keinen Sitz in der EU habe, seien die nationalen Behörden für Maßnahmen in ihrem eigenen Hoheitsgebiet zuständig.

Bei den durchgeführten Ermittlungen stellte die CNIL zwei Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) fest: Clearview verarbeitet die sensiblen biometrischen Daten demnach unrechtmäßig, da die Firma dafür keine Einwilligung einhole und auch keine andere infrage kommende rechtliche Basis vorliege. Zudem berücksichtige das Unternehmen Rechte der Betroffenen etwa auf Einsicht und zum Löschen ihrer Daten nicht zufriedenstellend und effizient.

Clearview extrahiert, so die CNIL, Fotos aus einer Vielzahl von Webseiten, sozialen Netzwerken und Videos. Auf diese Weise habe sich das Unternehmen weltweit über zehn Milliarden Bilder angeeignet. Mithilfe dieser Sammlung vermarkte es den Zugang zu seiner Bilddatenbank vor allem an Strafverfolger in Form einer App, in der eine Person mithilfe eines Fotos gesucht werden könne. Die Betroffenen rechneten realistischerweise aber nicht damit, dass ihre Bilder in ein Gesichtserkennungssystem eingespeist werden, „das von Staaten für polizeiliche Zwecke genutzt werden kann".

In Europa hatte zuletzt die britische Datenschutzbehörde ICO angekündigt gegen Clearview eine Geldstrafe in Höhe von rund 20 Millionen Euro verhängen zu wollen. Der frühere Hamburgische Datenschutzbeauftragte Johannes Caspar war ebenfalls bereits gegen die Firma vorgegangen. Kanadische Behörden haben Clearview gerade untersagt den Dienst in drei Provinzen weiter anzubieten und verpflichtet alle Bilder und Gesichtsdaten von deren Einwohnern zu löschen. Clearview vertritt den Standpunkt, die Bilder und Gesichtsdaten könnten gar nicht gelöscht werden, da sie keine Ortsangaben enthalten, obwohl die Identifikation der eigentliche Zweck sein sollte (s.u. S. 54, Krempl, Datenschützer: Clearview darf Gesichtsbilder von Franzosen nicht verarbeiten, www.heise.de 16.12.2021, Kurzlink: https://heise.de/-6297116; Schräer, Donnerstag: Gesichtserkennung in Kanada verboten, kein Geld mehr für DJI & Co, www.heise.de 16.12.2021, Kurzlink: https://heise.de/-6296471).

Schweiz

Neue DNA-Ermittlungskompetenzen

Die Strafverfolgungsbehörden in der Schweiz erhalten mehr Freiheiten bei der Erstellung von DNA-Profilen. Der Ständerat beschloss im September 2021, dass die Polizei künftig die mögliche Augen-, Haar- und Hautfarbe sowie die „biogeografische Herkunft" von unbekannten Personen aus Tatortspuren bestimmen darf (DNA-Phänotypisierung). Zudem soll in den DNA-Datenbanken nach biologischen Verwandten von Verdächtigen gesucht werden können. Zuvor hatte der Nationalrat trotz Mängeln die Vorlage durchgewunken, so dass der Ständerat Anpassungen vornehmen musste. So soll ein spezifischer Deliktkatalog mit schweren Gewaltverbrechen die Phänotypisierung und den Verwandtschaftssuchlauf beschränken. Die kleine Kammer verkürzte zudem die Löschfristen bei der Aufbewahrung der DNA-Profile und verlangt für bestimmte Fälle einen Gerichtsbescheid (GiD Nr. 259 November 2021, 30 f.).

Italien

Strafe gegen Apple und Google wegen ungenügender Werbeinformation

Die italienische Wettbewerbsbehörde Autorità garante della concorrenza e del mercato (AGCM) teilte am 26.11.2021 mit, dass sie Strafen in Höhe von jeweils 10 Mio. Euro gegen Apple und Google verhängt hat. Mit ihren Praktiken rund um die kommerzielle Verwendung von Nutzerdaten verstoßen demnach die Konzerne gegen Verbraucherrecht. Es handelt sich dabei um die derzeit in Italien mögliche Maximalstrafe für solche Verstöße. Für Apple ist es bereits die zweite Wettbewerbsstrafe in Italien innerhalb einer Woche.

Sowohl Apple als auch Google verwenden die Daten ihrer Nutzer für kommerzielle Zwecke. Apple gibt, so die AGCM, die Daten zwar nicht an Dritte weiter, setzt sie aber selbst zu Werbezwecken ein und zieht daraus einen unmittelbaren wirtschaftlichen Vorteil. Der Konzern schickt etwa Push-Nachrichten auf iPhones, um seine Abo-Dienste zu bewerben. Beide Konzerne würden die Sammlung und Verwendung der Nutzerdaten zu Werbezwecken allerdings nicht mit „klaren und unmittelbaren Informationen" deutlich machen. Beim Anlegen eines Apple- und Google-Accounts setzen beide Unternehmen zudem auf

„aggressive Praktiken“, um eine Erlaubnis zur kommerziellen Verwendung der Nutzerdaten einzuholen – etwa durch das Vorankreuzen bestimmter Felder, mit denen der Datenverwendung zugestimmt wird. Beides verstoße gegen italienische Verbraucherschutzgesetze.

Apple und Google haben vor die Entscheidung anzufechten. Apple bezeichnete die Einschätzung der Behörde als „falsch“. Man gebe den Nutzern Kontrolle darüber, welche Daten sie teilen wollen und wozu diese verwendet werden. Auch Google betonte in einer Stellungnahme, es würden „klare Informationen“ über die Verwendung der Nutzerdaten bereitgestellt (Becker, „Aggressive Praktiken“ bei Apple und Google: Regulierer verhängen Strafe, www.heise.de 26.11.2021, Kurzlink: https://heise.de/-6277945).

Norwegen

Hohes Bußgeld gegen Grindr wegen Datenweitergabe ohne Einwilligung

Die norwegische Datenschutzbehörde Norwegian Data Protection Authority (NO DPA) hat gemäß einer Mitteilung vom 15.12.2021 gegen die Betreiber der Mobile-Dating-App für Homosexuelle, Bi-, Trans- und Queer-Menschen Grindr ein Bußgeld in Höhe von 65 Mio. Norwegische Kronen (ca. 6,5 Millionen Euro) verhängt. Demnach hat Grindr gegen die Datenschutz-Grundverordnung (DSGVO) zur Einwilligung der Datennutzung der Anwender verstoßen. Grindr habe ohne das Einverständnis der App-Nutzer personenbezogene Daten für verhaltensbezogene Werbung an Dritte weitergegeben. Die Betreiber der Grindr-App haben es demnach versäumt von den Anwendern ausdrücklich die Genehmigung zur Weitergabe ihrer Daten an Dritte für verhaltensbezogene Werbung einzuholen. Das Akzeptieren der allgemeinen Datenschutzbestimmungen in ihrer Gesamtheit durch den Anwender, um die App nutzen zu können, reiche dafür nicht aus, weil dies einem Zwang einer Einwilligung zur Datenweitergabe gleichkomme. Die Weitergabe personenbezogener Daten seien dem Nutzer deshalb „nicht ordnungsgemäß“ mitgeteilt worden. Damit hätte Grindr im Zeitraum von Juli 2018 bis April 2020 keine gültige Einwilligung nach Maßgabe der DSGVO eingeholt. Der aktuelle Zustimmungsmechanismus sei nicht Gegenstand der Untersuchung gewesen.

2020 hatte die Norwegische Verbraucherschutzbehörde (Norwegean Consumer Council) eine Beschwerde gegen Grindr eingelegt, nach der Grindr personenbezogene Daten zu Marketingzwecken unrechtmäßig an Dritte weitergegeben hat. Darunter haben sich GPS-Ortsdaten des Nutzers, die IP-Adresse, Werbe-ID, das Alter und Geschlecht sowie Informationen, die den Anwender als Grindr-Nutzer ausweisen, befunden. Nach Ansicht der NO DPA könnten Nutzer anhand dieser Daten identifiziert werden und die Daten konnten weitergeben werden.

Die NO DPA betont, dass diese Daten einen Grindr-Nutzer als Angehörigen einer sexuellen Minderheit ausweisen können. Grindr-Nutzer würden die App mitunter anonym nutzen wollen ohne etwa den eigenen Namen vollständig anzugeben oder ein Foto von sich hochzuladen. Informationen, die die sexuelle Ausrichtung eines Menschen betreffen, unterliegen aber einem besonderen Schutz. Trotzdem, so Tobias Judin, Leiter der NO DPA, wurden diese und weitere persönliche Daten an Dritte zu Marketingzwecken weitergegeben.

Die NO DPA sieht in dem Verstoß einen besonders schwerwiegenden Fall, der ein abschreckendes hohes Bußgeld rechtfertigt. Grindr habe die Daten von Tausenden norwegischen Nutzenden aus kommerziellem Interesse weitergegeben. Ursprünglich sollte die Strafe 100 Millionen Norwegische Kronen betragen. Bei der Verhängung des Bußgeldes wurden jedoch die finanzielle Lage des Unternehmens und der Umstand berücksichtigt, dass die beanstandeten Mängel zur Einwilligung schnell behoben wurden. Grindr kann innerhalb von drei Wochen nach Erhalt der Entscheidung widersprechen. Diese Frist könne auch verlängert werden (Bünte, DSGVO-Verstoß: Norwegische Datenschützer verhängen Millionenstrafe gegen Grindr, www.heise.de 15.12.2021, Kurzlink: https://heise.de/-6295438)

Polen

Schwangerschaften werden zum zu kontrollierenden Sicherheitsrisiko

Polens Staatsanwaltschaft und Geheimdienste sollen künftig kontrollieren, ob Polens Frauen schwanger sind, sie nach neun Monaten ein Baby zur Welt bringen oder aber eine Fehlgeburt erleiden. Die dies regelnde Verordnung der nationalpopulistischen Regierung der Partei Recht und Gerechtigkeit (PiS) trat am 01.01.2022 in Kraft.

Schon bisher haben alle Patienten und Patientinnen in Polen eine individuelle Patientenkarte im Internet. Diese Daten sind – zumindest theoretisch – durch die Schweigepflicht der Ärzte geschützt. Doch nun sollen zahlreiche persönliche Daten, darunter auch Schwangerschaften, in einem medizinischen Zentralregister erfasst werden, auf das Staatsanwaltschaft und Geheimdienste jederzeit Zugriff hätten. Gemäß dem Senator der liberalen Bürgerkoalition (KO), Krzysztof Brejza, gehen die Änderungen auf die Initiative des PiS-Gesundheitsministeriums und des Chefs des Justizministeriums und der Staatsanwaltschaft Zbigniew Ziobro zurück. Nach der Veröffentlichung der Pläne brach auf Twitter ein Aufruhr los. Sarkastisch kommentierte die feministische „Bewegung der acht Sternchen“: „Super! Und wenn ein Paar sich ein Kind wünscht, die Frau dann aber eine Fehlgeburt erleidet, muss sie vor dem Staatsanwalt erklären, dass sie das Kind wirklich wollte.“ Eine Userin namens Agata Nowak schrieb: „Versteht Ihr, was hier passiert? Eure Schwangerschaft wird kein intimes Erlebnis zwischen Dir, Deinem Partner und dem behandelnden Arzt sein. Der Staatsanwalt erfährt sofort davon und alle Beamten, die Zugriff auf das Register haben: Vorname, Name, Geburtstermin. Ihr werdet sein wie kalbende Kühe.“ Zum Schluss startete sie einen Aufruf: „Auf die Straße, Leute!“ Eine Johanna befürchtet, dass auch das den Radikalen in der PiS wohl nicht weit genug gehen wird: „Demnächst werden sie noch alle Verhütungsmittel verbieten!“

In Polen gilt eines der strengsten Abtreibungsgesetze Europas. Ende 2020 urteilte das von der PiS kontrollierte Verfassungsgericht Polens, dass ein schwer fehlgebildeter oder nicht überlebensfähiger Fötus keine medizinische Indikation für eine legale Abtreibung darstelle. Dies sei unvereinbar mit Polens Verfassung. Den Antrag auf Überprüfung des Abtreibungsrechts hatten einige Abgeordnete der regierenden PiS gestellt, und dies gegen den klaren Willen der Bevölkerungsmehrheit, wie mehrere Umfragen zeigten. Seither sind legale Abtreibungen nur noch bei einer Gefahr für die Gesundheit oder das Leben der Schwangeren oder bei Vergewaltigung möglich. Die offizielle Statistik müsste demnach schon für 2021 auf weit unter 1.000 legale Abtreibungen fallen, und dies bei einer Gesamtbevölkerung von 38 Mio. Einwohnern. Gynäkologen stehen bei Risikogeburten nun vor dem Dilemma zu entscheiden, ab wann das Leben des Fötus keinen Vorrang mehr vor dem Leben der Schwangeren hat. So wird von einem Fall berichtet, bei dem die Ärzte zu lange darauf gewartet hatten, dass keine Herztöne des Fötus mehr zu hören waren, und erst dann einen Kaiserschnitt eingeleitet. Die junge Frau, die bereits Mutter eines kleinen Mädchens war, starb an einer Blutvergiftung (Lesser, Uterus unter staatlicher Aufsicht, https://taz.de/Familienpolitik-in-Polen/!5809678/ 08.12.2021).

Polen

Opposition mit Pegasus ausgespäht

Der polnische Ministerpräsident Mateusz Morawiecki hatte es zunächst als „Fake News" bezeichnet, als der Verdacht aufkam, seine Regierung habe politische Gegner mit der Pegasus-Software ausgespäht und so den Ausgang der Parlamentswahl im Herbst 2019 beeinflusst. Dokumente des Obersten Rechnungshofs in Polen geben nun Hinweise darauf, wie der Ankauf der Software im September 2017 im Sejm vonstatten ging und wie dies vor den Abgeordneten verschleiert wurde.

Drei Personen sollen ausgespäht worden sein: die Staatsanwältin Ewa Wrzosek, der Anwalt Roman Giertych und der Senatsabgeordnete Krzysztof Brejza. Letztgenannter hatte 2019 den Wahlkampf der liberalkonservativen Bürgerkoalition KO geleitet, an deren Spitze heute Oppositionsführer Donald Tusk steht. Die Abhöraktion während des Wahlkampfs zeige, so Brejza, „dass Einfluss auf das Fundament der Demokratie genommen wurde". Tusk sprach von „der tiefsten und schwersten Krise der Demokratie seit 1989" und zog einen Vergleich zur Watergate-Affäre, über die US-Präsident Nixon 1972 stürzte.

Brejza ist sicher, dass die Wahl 2019 anders ausgegangen wäre, wenn nicht sein Smartphone gehackt worden wäre. Der PiS-nahe Fernsehsender TVP hatte damals manipulierte SMS von Brejza präsentiert und den Eindruck erweckt, Brejza koordiniere Hasskampagnen gegen die politischen Gegner. Nach heftigen Attacken auf ihn gab Brejza den Job als Kampagnenleiter auf. In sozialen Netzwerken präsentierte Brejza nun Original und Fälschung der Nachrichten; er hatte sich damals nicht erklären können, wie TVP an seine SMS gekommen war. Im Oktober 2021 vermutete er, mit Pegasus ausgespäht worden zu sein. Seine Vermutung bestätigte sich kurz vor Weihnachten.

Gemäß einer Untersuchung des kanadischen Forscherteams Citizen Lab von der Universität Toronto wurde Brejzas Smartphone 33-mal zwischen April und Oktober 2019 angegriffen. Die Software, entwickelt von der israelischen NSO Group, ermöglicht es Angreifern Nachrichten, Fotos, Passwörter und Browserverläufe abzuschöpfen; sie kann zudem unbemerkt Kamera und Mikrofon auf den Geräten anschalten (vgl. DANA 4/2021, 239 ff., DANA 3/2021, 187 ff.). Das Telefon des Anwalts Giertych, zu dessen Mandanten hochrangige Oppositionelle gehören, wurde ebenfalls vor der Wahl 2019 18-mal angegriffen.

Das Handy der Staatsanwältin Ewa Wrzosek wurde im Sommer 2021 gehackt. Wrzosek machte sich unbeliebt, weil sie im Frühjahr 2020 gegen eine vorgezogene Präsidentschaftswahl vorging. Sie engagiert sich gegen die Justizreformen der Regierungspartei PiS, welche laut der EU-Kommission die Rechtsstaatlichkeit in Polen untergraben. Vor allem kämpft Wrzosek für die Unabhängigkeit der Staatsanwaltschaft. Wegen ihres Engagements wurde Wrzosek bereits einmal strafversetzt. In der Hacking-Affäre hat sie Anzeige erstattet, allerdings lehnte es die Staatsanwaltschaft ab ein Verfahren einzuleiten. Begründung: Wrzosek wolle ihr Mobiltelefon nicht aushändigen. Den Medien sagte die Juristin, sie hätte das Gerät zur Verfügung gestellt, sobald Ermittlungen aufgenommen würden. In früheren Fällen waren Beweismittel verschwunden.

Donald Tusk erklärte am 04.01.2022, dass seine Partei PO die Einsetzung einer Untersuchungskommission beantragen werde, um den Einsatz der Pegasus-Software aufzuklären. Regierungssprecher Piotr Müller erwiderte, er sehe für eine solche Kommission keinen Grund. Wer Zweifel habe, solle sich an die Staatsanwaltschaft wenden. Zuvor hatte ein Abgeordneter der Opposition einem Zeitungsorgan ein Dokument des Rechnungshofes übergeben, durch das sich nachvollziehen lässt, wie Pegasus für etwa 5,4 Millionen Euro im Jahr 2017 eingekauft wurde. Demnach wurde die Anschaffung für den Geheimdienst gesetzeswidrig aus der falschen Kasse bezahlt. Vor allem aber wurde der Einkauf offenbar bewusst vor Abgeordneten und Beamten verschleiert. So billigten sie ihn ohne von der Verwendung zu wissen. Der Name des Fonds, über den der Einkauf lief: Opferhilfe und Bekämpfung von Kriminalitätsfolgen.

Derweil wies Jaroslaw Kaczynski, Polens Vize-Ministerpräsident, die Berichte zurück und erklärte, es wäre schlecht, wenn Polens Geheimdienste nicht mit einem Instrument wie Pegasus ausgestattet wären. Aber die „Geschichten der Opposition, dass Pegasus zu politischen Zielen eingesetzt wurde, sind völliger Unfug" (Viktoria Grossmann, Ausgespäht mit Pegasus, SZ 05./06.01.2022; Kaczynski wehrt sich, SZ 08./09.01.2022, 6).

Polen

Wettbewerbsbehörde geht gegen Apples Tracking-Initiative vor

Die polnische Wettbewerbsbehörde Urząd Ochrony Konkurencji i Konsu-

mentów (UOKiK) nimmt Apples Vorgaben zu Werbe-Tracking in Apps unter die Lupe und prüft, ob die in iOS integrierte Funktion auf ein „Eliminieren von Konkurrenten im Markt für personalisierte Werbung“ ausgelegt ist. Die Untersuchung soll klären, ob ein Missbrauch von Marktmacht zum Ausschluss von Wettbewerb vorliegt.

iPhone-Apps müssen seit iOS 14.5 für ein Anbieter-übergreifendes Werbe-Tracking beim Nutzer erst um Erlaubnis fragen. Nur dann gibt das Betriebssystem den Zugriff auf die integrierte Werbe-ID frei, die so auch das Anlegen von Profilen und das Beobachten von Aktivitäten über Apps hinweg ermöglicht. Apples Regeln für App-Anbieter haben deren Möglichkeiten zum Sammeln von Daten für personalisierte Werbung erheblich reduziert, so die Regulierungsbehörde. Dabei geht es vor allem um die Frage, ob Apple dadurch zugleich das eigene Werbegeschäft gestärkt hat.

Apples Tracking-Transparenz-Initiative ist in der Werbebranche auf erheblichen Widerstand gestoßen. Besonders Werberiesen wie Facebook, deren Tracking-Technik auf der Werbe-ID aufbaute, sahen eine Beeinträchtigung ihres Geschäftes. Schätzungen zufolge haben Social-Media-Plattformen Werbeumsätze in Milliardenhöhe durch die Tracking-Nachfrage in iOS verloren. Auch erste werbende Unternehmen haben in den letzten Wochen beklagt, die Neukundengewinnung auf iPhones sei schwieriger und kostspieliger geworden.

Auch in Frankreich hatten Werbeverbände eine Kartellbeschwerde gegen die Apple-Initiative eingereicht. Es handele sich dabei aber um „keine missbräuchliche Handelspraktik“, entschied die Autorité de la Concurrence im Frühjahr 2021. Man wolle dies aber weiter untersuchen, um sicherzustellen, dass es zu keiner Selbstbevorzugung kommt. Bemängelt wurde unter anderem, dass Apple bei seinem eigenen Werbedienst auf ein Opt-in verzichtet; inzwischen wird dafür aber um Erlaubnis gebeten (Becker, Datenschutz gegen Wettbewerb: Polnische Regulierer prüfen Apple, www.heise.de 13.12.2021, Kurzlink: https://heise.de/-6293881).

Großbritannien

Sammelklage gegen Meta geplant

Die Wettbewerbsexpertin Liza Lovdahl-Gormsen vom British Institute of International and Comparative Law teilte mit, dass sie in Zusammenarbeit mit Anwälten eines Klagefonds für 44 Millionen Nutzerinnen und Nutzer über eine Sammelklage gegen die dortige Niederlassung von Facebooks Muttergesellschaft Meta Schadenersatzforderungen erstreiten möchte; insgesamt könnten nach ihrer Ansicht die Forderungen bis zu einer Höhe von 2,756 Milliarden Euro gehen. Das Unternehmen habe seine „marktbeherrschende Stellung missbraucht“, um den britischen Nutzern Bedingungen für die Nutzung persönlicher Daten zu diktieren. Mit den im Zeitraum von 2015 bis 2019 gesammelten Daten habe Facebook ein detailliertes Bild der Internetnutzung der Betroffenen erhalten und „übermäßige Gewinne“ erzielt.

Lovdahl-Gormsen bemängelt dabei unter anderem „Facebook Pixel“ – JavaScript-Code für Webseitenbesitzer, mit dessen Hilfe sich das Nutzungsverhalten der Seitenbesucher tracken lässt. Jeder, der in Großbritannien lebt und Facebook im besagten Zeitraum mindestens einmal genutzt habe, kann nach Ansicht von Lovdahl-Gormsen Schadenersatz von Facebook fordern.

Für den Erfolg der gemeinsam mit einer erfahrenen britischen Anwaltskanzlei geplanten Sammelklage gibt es keine Garantie. Der Londoner Supreme Court hatte im November 2021 bereits eine Klage gegen Google zurückgewiesen. In dem Fall wurde Google beschuldigt Millionen iPhones illegal überwacht zu haben. Eine weitere Sammelklage gegen Google von einem britischen Verband für das Umgehen der Cookie-Sperre von Apples Safari-Browser wurde 2018 ebenfalls zurückgewiesen (Koch, Datenschutz: Facebook droht Sammelklage in Großbritannien, www.heise.de 14.01.2022, Kurzlink: https://heise.de/-6327433).

Großbritannien

Weiter Gerichtsstreit um Datenbeschaffung durch „The Sun“

Im August 2005 rief Rebekah Brooks, die damalige Chefin der britischen Boulevardzeitung „The Sun“, den Agenten der Schauspielerin Sienna Millers an und fragte, ob man sich mit ihr mal über deren Schwangerschaft unterhalten könne. Zu diesem Zeitpunkt hatte Miller noch nicht einmal ihrer Familie oder ihren engsten Freunden von besagter Schwangerschaft erzählt. Vor dem Londoner High Court wirft nun Miller „The Sun“ vor, die Zeitung habe sie so gezwungen, Entscheidungen „über meinen eigenen Körper zu treffen, mit denen ich jeden Tag leben muss“.

Miller hatte nach einem Vergleich mit Rupert Murdochs Firma „News Group Newspapers“, die „The Sun“ herausgibt, eine erhebliche finanzielle

Abfindung akzeptiert. Der High Court entschied nun nach einem Einspruch von Murdochs Anwälten über die genaue Formulierung des Statements, das Miller und ihr Anwaltsteam nach dem Vergleich veröffentlichen wollten, also auch darüber, welche Vorwürfe die Schauspielerin explizit wiederholen darf.

Miller wirft dem Journalisten Nick Parker, der weiterhin für „The Sun" arbeitet, vor ihre privaten Krankenakten über eine Mittelsfrau illegal an sich gebracht und so von ihrer Schwangerschaft erfahren zu haben. Parker bestreitet das. Miller wiederholte zudem, sie sei überzeugt, dass ihre Freunde und Familie „dem anhaltenden, umfangreichen und gezielten Abfangen von Voicemails und rechtswidrigen Informationsbeschaffungsaktivitäten durch Journalisten der Sun" ausgesetzt waren. Laut Miller, die das Baby letztlich nicht bekam, sei ihr versichert worden, dass die Zeitung diese Informationen über ihre Schwangerschaft nicht publizieren werde. Letztlich seien sie aber dennoch abgedruckt worden. Ihr Leben sei dadurch fast ruiniert worden. Das sei so weit gegangen, dass sie ihrer Familie und Freunden vorgeworfen habe Informationen an „The Sun" verkauft zu haben. Die Zeitung streitet die Vorwürfe ab und versuchte Miller mit juristischen Mitteln daran zu hindern, sie zu wiederholen. Das Gericht entschied aber, dass Miller das zumindest teilweise darf.

Dies ist auch nicht der erste juristische Konflikt zwischen Sienna Miller und einer Murdoch-Zeitung. 2011 erhielt sie im Rahmen der Untersuchungen zum Abhörskandal um die mittlerweile eingestellte Sonntagszeitung „News of the World" vom High Court Schmerzensgeld in Höhe von 100.000 Pfund zugesprochen. Die „News of the World" mussten damals zugeben illegal ihr Telefon gehackt zu haben.

Im aktuellen Fall haben News Group Newspapers allerdings keinerlei Schuld eingestanden. Die Linie des Medienunternehmens lautet, während der 2000er-Jahre, als Rebekah Brooks Chefredakteurin der „News of the World" war, sei Telefon-Hacking dort zwar weit verbreitet gewesen, nach Brooks' Wechsel zum Schwesterblatt „Sun" 2003 hätten dort jedoch keine illegalen Aktivitäten stattgefunden. Dessen ungeachtet zahlte das Unternehmen immer wieder hohe Summen an Personen, die der „Sun" rechtswidrige Informationsbeschaffung vorwarfen. Dazu gehörten der Fußballer Paul Gascoigne, der ebenfalls Mitte Dezember 2021 einem Vergleich mit der „Sun" zustimmte. Laut Gascoigne hatte die Veröffentlichung persönlicher medizinischer Informationen „verheerende und schwächende Auswirkungen" auf seine psychische Gesundheit und sein Wohlbefinden.

Miller hat nach eigenen Aussagen dem Vergleich zugestimmt, weil ihr die finanziellen Mittel fehlen, um ein Gerichtsverfahren gegen das Murdoch-Imperium anzustrengen. Sie sei jedoch bereit in jedem zukünftigen Verfahren gegen die „Sun" gerne auszusagen: „In diesem Verfahren habe ich aus erster Hand erfahren, wie weit diese Zeitung und dieses Unternehmen gehen, um ihre Spitzenkräfte vor Entlarvung zu schützen und davor, die Konsequenzen ihres Handelns zu spüren zu bekommen." Die Aufmerksamkeit wendet sich nach diesem Vergleich Prinz Harry zu. Dieser wirft der „Sun" vor das Telefon seiner Frau Meghan Markle abgehört zu haben. Im Gegensatz zu Sienna Miller hätten der Herzog von Sussex und seine Frau die nötigen Mittel für ein Gerichtsverfahren (vgl. DANA 2/2011, 88 f., 1/2012, 29 f.; 4/2015, 184, 1/2018, 48, Menden, Wie erfuhr die „Sun" von Sienna Millers Schwangerschaft? SZ 13.12.2021, 19, https://www.sueddeutsche.de/medien/sienna-miller-sun-1.5485415).

Türkei

Gericht hebt Filmverbot bei Polizeieinsätzen auf

Die türkische Polizei ist mit dem Versuch gescheitert Videoaufnahmen von ihren Einsätzen bei Demonstrationen zu verbieten. Das Oberste Verwaltungsgericht erklärte eine entsprechende Anordnung der Polizeidirektion für nichtig. Die Ende April 2021 publik gewordene Anordnung sah vor, dass Ton- und Bildaufnahmen von Einsatzkräften bei Demonstrationen unterbunden werden sollen. Mehrere Anwaltskammern hatten Beschwerde eingelegt. In der Gerichtsentscheidung wurde nun zur Begründung genannt, dass die Anordnung die Pressefreiheit einschränke und gegen die Verfassung verstoße. Grundfreiheiten könnten allenfalls per Gesetz eingeschränkt werden, nicht aber von der Polizei. Innenminister Süleyman Soylu hatte die Anweisung verteidigt: „Hier liegt weder ein Verstoß gegen die Verfassung noch gegen die Demokratie vor" (Filmverbot von Polizei aufgehoben, www.jungewelt.de 13.11.2021; Kein Filmverbot für Polizeieinsätze, Kieler Nachrichten, 15.11.2021, 7).

Israel

Späh-Software-Export-beschränkungen nach „Pegasus"-Berichten

Das Verteidigungsministerium Israels teilte mit, dass das Land die Vorschriften für den Export von Cybertechnologie verschärft hat, um sicherzustellen, dass zum Beispiel bestimmte Spionagesoftware tatsächlich nur noch zur Verhinderung von Terrorakten und schweren Straftaten eingesetzt wird. Israels Regierung reagiert damit offensichtlich auf die Recherchen des „Pegasus-Projekts", bei dem ein internationales Journalistenkonsortium einen weit verbreiteten Missbrauch der Spähsoftware des israelischen Unternehmens NSO aufgedeckt hatte. Hunderte Aktivisten, Journalisten und Politiker bis hinauf zu Frankreichs Präsident Emmanuel Macron waren dabei offenbar zum Ziel dubioser Abhörmanöver geworden (DANA 3/2021, 187 f, 4/2021, 239 ff.).

Israels Regierung, die den Export solcher Cybertechnologie in jedem einzelnen Fall genehmigen muss, war nach den Veröffentlichungen im Sommer 2021 unter erheblichen Druck geraten. Verteidigungsminister Benny Gantz hatte bei einem Besuch in Frankreich Rede und Antwort zur Abhör-Affäre stehen müssen. Bundeskanzlerin Angela Merkel sprach sich für eine Verkaufsbeschränkung solcher Spähsoftware aus. Das US-Handelsministerium setzte schließlich das Unternehmen NSO auf eine Sanktionsliste. Zuletzt war Anfang Dezember 2021 bekannt geworden, dass auch Mitarbeiter des US-Außenministe-

riums in Afrika zum Opfer der Pegasus-Software geworden waren.

Die neuen israelischen Export-Richtlinien, die von einem Team des Verteidigungs- und des Außenministeriums gemeinsam formuliert worden sind, geben nun konkreter vor, wo solche Cybertechnologie eingesetzt werden darf: „Die Definitionen für schwere Straftaten und terroristische Handlungen wurden verschärft, um zu verhindern, dass die Grenzen in diesem Zusammenhang verwischt werden." Ausdrücklich festgehalten wird, dass „Meinungsäußerungen oder Kritik" nicht in die Kategorien Terror- oder Straftaten fallen. Verboten wird der Einsatz solcher Späh-Programme gegen einzelne Personen oder Gruppen aufgrund ihrer Religion, ihrer sexuellen Orientierung, ihrer ethnischen Zugehörigkeit oder ihrer politischen Einstellung. Alle Staaten, die israelische Cybertechnologie erwerben wollen, müssen eine entsprechende Erklärung unterzeichnen. Wer die Vorgaben missachtet, dem soll die Lizenz zur Nutzung entzogen werden.

Zuvor hatte bereits ein israelisches Wirtschaftsmagazin berichtet, dass die Liste der Länder, in die israelische Cybertechnologie exportiert werden darf, von 102 auf 37 Staaten reduziert worden sei. Auf der Liste sollen sich dem Bericht zufolge vor allem noch westeuropäische Länder sowie die USA und Kanada befinden, aber nicht mehr Staaten wie Ungarn, die Vereinigten Arabischen Emirate, Saudi-Arabien oder Marokko, in denen nach Recherchen des Pegasus-Projekts grober Missbrauch mit der Spähsoftware getrieben wurde. Zumindest in der Vergangenheit hatte Israels Regierung den Verkauf von Cybertechnologie gezielt auch als diplomatischen Türöffner genutzt. So gab es vorab Exportgenehmigungen in jene arabischen Staaten, mit denen später im Abraham-Abkommen eine Normalisierung der Beziehungen vereinbart wurde.

Der Jerusalemer Menschenrechtsanwalt Eitay Mack, der seit vielen Jahren die israelische Exportpraxis in diesem Bereich kritisiert, hält jedoch auch die neuen Regelungen für wenig hilfreich. Er vermutet einen „Bluff" und eine „PR-Show", mit der allein dem internationalen Druck nach der Aufregung über die Pegasus-Recherchen ausgewichen werden soll: „Mit dem neuen Formular unterschreibt ein Diktator, dass er kein Diktator ist." Ob ein Menschenrechtler oder ein Journalist eine Bedrohung darstellt, könnten solche Regime auch unter den neuen Vorgaben auf ihre Weise definieren.

Die Kritik an Pegasus dürfte Auswirkungen auf die Geschäfte der NSO-Group haben: Pegasus ist bisher der größte Geschäftsbereich des Unternehmens und steht laut Presseberichten für etwa die Hälfte des Umsatzes, der für 2021 mit rund 230 Mio. US-Dollar beziffert wird.

Derweil denkt die NSO Group Medienberichten zufolge – unter Berufung auf Verhandlungskreise – über einen Verkauf nach und spricht offenbar mit möglichen Investoren. Dabei stehe auch eine Neuaufstellung des Unternehmens zur Diskussion. Die finanzielle Situation des Unternehmens scheint angespannt zu sein. Die Mitgründer Shalev Hulio und Omri Lavie hatten die Mehrheitsanteile an der Firma 2019 vom Investor Francisco Partners zurückgekauft. Die NSO Group wurde dabei mit rund einer Milliarde US-Dollar bewertet. Zur Finanzierung hatten die Gründer Schulden in Höhe von mehreren hundert Millionen US-Dollar aufgenommen. Mit Investmentfonds werde eine Refinanzierung erörtert, aber auch ein Verkauf und eine Restrukturierung stehen im Raum. Dabei könnte die Entwicklung von Pegasus eingestellt und NSO auf Cyberabwehrsysteme und Drohnentechnologie ausgerichtet werden. Das Unternehmen und die beteiligten Finanzhäuser kommentierten die Berichte nicht (Münch, Export von Späh-Software erschwert, SZ 08.12.2021, 9; Brieglеb, Spyware: Ausverkauf bei NSO Group – das Ende von Pegasus? www.heise.de 14.12.2021, Kurzlink: https://heise.de/-6294818).

Israel

Pegasus-Einsatz gegen Palästinenser-NGOs?

Sicherheitsforscher von Amnesty International (AI) haben die umstrittene Malware Pegasus auf Handys von sechs palästinensischen Menschenrechtlern aus Nichtregierungsorganisationen (NGOs) gefunden. Gemäß der Menschenrechtsorganisation AI und dem „Citizen Lab" der Universität von Toronto stehen die betroffenen Aktivisten teils in Verbindung mit palästinensischen Menschenrechtsgruppen, die Israel in einem umstrittenen Schritt jüngst zu Terrororganisationen erklärt hatte. Es handelt sich um die ersten bekannten Fälle von Nachweisen der Spähsoftware der NSO Group mit Sitz in Tel Aviv bei palästinensischen Aktivisten.

Zuvor war bekannt geworden, dass vor allem autoritäre Regierungen die Überwachungssoftware im großen Stil gegen Kritiker, Oppositionelle und Journalisten einsetzten (DANA 3/2021, 187 ff.). Das Programm setzt sich in Smartphones fest und sammelt Orts- und persönliche Daten der Smartphone-Nutzer. Es kann auch auf Mikrofone und Kameras von Mobiltelefonen zugreifen.

Mohammed Maskati von der Non-Profit-Organisation Frontline Defenders meinte, es sei zunächst unklar, wer die Telefone der palästinensischen Aktivisten infiltriert habe. Die Gruppe mit Sitz in Irland und mindestens zwei der Betroffenen sagten, sie vermuteten, dass der Staat Israel dahinterstecke.

Kurz nach dem Nachweis der ersten zwei Infiltrationen Mitte Oktober 2021 hatte der israelische Verteidigungsminister Benny Gantz sechs Organisationen der palästinensischen Zivilgesellschaft zu Terrororganisationen erklärt. Israel hat bislang kaum Belege erbracht, um die angeblichen Verbindungen der Menschenrechtsgruppen zum Terrorismus nachzuweisen. UN-Menschenrechts-Kommissarin Michelle Bachelet sprach von einer „willkürlichen Entscheidung", AI und Human Rights Watch von einem „erschreckenden und unrechtmäßigen Akt", linke israelische Gruppierungen gar vom „Handeln totalitärer Regime". Das Büro des israelischen Premierministers und das israelische Verteidigungsministerium bestritten die Pegasus-Software derart eingesetzt zu haben.

Mit der Einstufung von sechs Nichtregierungsorganisationen als Terrorgruppen hat Israels Regierung mitten hinein gezielt ins Zentrum der palästinensischen Zivilgesellschaft und sich damit zugleich dem Vorwurf ausgesetzt unbequeme Kritiker der Besatzungspolitik zum Schweigen bringen zu wollen.

Alle diese Organisation, die teils Geld auch aus europäischen Staaten, von der EU oder von deutschen Stiftungen bekommen, stehen seit Langem schon im Fokus der israelischen Behörden. Ihre Büros waren teils wiederholt Ziel von Durchsuchungen durch die Armee. Der pauschale Vorwurf, als „organisiertes Netzwerk" und Finanzierungsquelle der marxistischen Volksfront für die Befreiung Palästinas (PFLP) zu operieren, kam dennoch überraschend und wird von allen aufgelisteten Organisation heftig dementiert. Mit einer speziellen Anordnung kann Israels Armee sofort gegen die Organisationen im Westjordanland vorgehen und zum Beispiel ihre Büros schließen und Beschäftigte verhaften.

Das Thema führte auch zu Zoff innerhalb der israelischen Regierung. Meretz und Arbeitspartei, die beiden linken Parteien in der gegenwärtig regierenden heterogenen Acht-Parteien-Koalition, übten heftige Kritik und verlangten die Vorlage von Beweisen für den Terrorvorwurf.

Die prominenteste NGO auf der israelischen Terrorliste ist die seit 1979 aktive NGO Al-Haq unter ihrem Direktor Shawan Jabarin, der in den Achtziger- und Neunzigerjahren mehrfach wegen des Vorwurfs von PFLP-Aktivitäten in israelischer Haft saß. Den besonderen Ärger der israelischen Führung hatte sich Al-Haq mit einer Dokumentation mutmaßlicher israelischer Verbrechen eingehandelt, die dem Internationalen Strafgerichtshof in Den Haag (ICC) vorgelegt wurde. Der ICC ermittelt inzwischen wegen möglicher Kriegsverbrechen gegen Israel und die palästinensische Hamas. Al-Haq prangert jedoch nicht nur Menschenrechtsverletzungen der israelischen Besatzungsmacht an, sondern legt sich immer wieder mit der zunehmend autoritären Palästinensischen Autonomiebehörde von Präsident Mahmud Abbas an.

Seit drei Jahrzehnten aktiv und international vernetzt ist auch die Organisation Addameer, die Rechtshilfe für palästinensische Häftlinge in israelischen Gefängnissen anbietet. Speziell um palästinensische Kinder in israelischer Haft sowie allgemein um die Auswirkungen der Besatzung auf die Rechte von Kindern kümmert sich die palästinensische Sektion von Defense for Children International (DCI-P). Das Hauptquartier der Organisation liegt in Genf. Aufgelistet wurden von Israels Regierung zudem noch das sozial engagierte Bisan Center sowie zwei Organisationen, die sich eigenen Angaben zufolge für Frauenrechte (Union of Palestinian Women's Committees) und für die Stärkung der palästinensischen Landwirtschaft (Union of Agricultural Work Committees) einsetzen.

Zum Beleg der angeblichen Terroraktivitäten verweist Israel auf geheimdienstliche Erkenntnisse. Öffentlich wurden jedoch keinerlei Beweise vorgelegt. Auch die Dokumente, die den Partnern in den USA und in der Europäischen Union hinter den Kulissen vorgelegt wurden scheinen bislang wenig Überzeugungskraft zu haben. „Mehr Informationen" hatte ein Sprecher des US-Außenministeriums bereits unmittelbar nach der israelischen Bekanntmachung vom 22.10.2021 verlangt. Ein EU-Sprecher verwies umgehend darauf, dass bereits in der Vergangenheit israelische Vorwürfe über den Missbrauch von EU-Geldern durch palästinensische Organisationen „nicht fundiert" gewesen seien. Damit bezog er sich offenkundig auf ein vom israelischen Inlandsgeheimdienst Schin Bet zusammengestelltes 74-seitiges Dossier, das bereits im Mai 2021 an westliche Partner geschickt worden war. Der einhellige Befund: keine harten Beweise.

Kurz vor der Offenlegung dieser Pegasus-Infektion hatte die US-Regierung Joe Bidens gegen die NSO Group und die ebenfalls israelische Firma Candiru Exportbeschränkungen verhängt. Das US-Handelsministerium teilte mit, sie würden in die Liste der Unternehmen aufgenommen, deren Zugang zu US-Komponenten und US-Technologie eingeschränkt ist und die staatliche Genehmigungen für den Export benötigen. Die NSO Group und drei weitere Unternehmen, die nun ebenfalls auf der Sanktionsliste stehen, hätten Werkzeuge zur Verfügung gestellt, um länderübergreifende Repressionen umzusetzen (s.u. S. 53).

Auf die Vorwürfe hinsichtlich der Beschattung der palästinensischen Aktivisten angesprochen, erwiderte die NSO Group in einer Mitteilung, das Unternehmen identifiziere seine Kunden aus vertraglichen Gründen und zur Wahrung nationaler Sicherheitsinteressen nicht. Informationen, wer mit den Programmen der Firma gehackt werde, erhalte das Unternehmen nicht, es verkaufe diese aber nur an Regierungsbehörden für die Nutzung gegen „ernste Kriminalität und Terrorismus" (Spähsoftware Pegasus bei palästinensischen Aktivisten entdeckt, www.zeit.de 08.11.2021; Münch/Obermaier/Obermeyer, Pegasus-Einsatz gegen Palästinenser, SZ 09.11.2021, 6)

Israel

Ultraorthodoxe Rabbiner verteidigen „koschere Handys"

Sittenstrenge ultraorthodoxe Rabbiner haben schon manchen Feldzug gegen das Smartphone geführt – mit Worten oder gar mit dem Hammer, der z.B. direkt auf ein böses iPhone niedersauste. Der frommen Gefolgschaft sind nur „koschere Handys" erlaubt, ohne Zugang zum Internet, das als Ort der Sünde gilt. Über die Einhaltung der Regeln wacht ein eigens geschaffenes „Rabbinisches Komitee für Kommunikationsangelegenheit". Zwischen Israels Regierung und den Religionsführern hat sich nun deswegen eine heftige Auseinandersetzung entwickelt. Der Kampf ums koschere Handy ist voll entbrannt, weil Kommunikationsminister Yoaz Hendel eine weitere Deregulierung des Mobilfunkmarkts plant. Seit 2007 können Israelis beim Wechsel des Anbieters ihre alte Telefonnummer mitnehmen. Ausgenommen davon sind bislang die Besitzer der geschätzt rund 500.000 koscheren Mobiltelefone, die über besondere Nummern verfügen. Diese Ausnahme soll nun gestrichen werden, was für die Rabbiner Kontrollverlust bedeutet.

Die Aufsicht des Rabbiner-Komitees über die Handys geht weit über die Verhinderung des Internetzugangs hinaus. Geblockt wird zum Beispiel eine lange Liste von Telefonnummern. Für reichlich Kritik sorgte dabei immer wieder, dass darunter nicht nur Sexanbieter sind, sondern auch Informationsstellen der Regierung, Notrufnummern für Opfer von sexueller Gewalt oder Bera-

tungsstellen für diejenigen, die aus der ultraorthodoxen Gemeinschaft aussteigen wollen.

Über das koschere Handy lässt sich also steuern, mit wem die Nutzenden kommunizieren und welche Information sie erreichen. Die Telefonnummer ist dabei zu einem Ausweis der frommen Gefolgschaft geworden. Dies fällt weg, wenn die Nummern künftig bei einem Anbieterwechsel unkontrolliert auch für Smartphones genutzt werden können. In einem offenen Brief haben daher der sephardische und der aschkenasische Chefrabbiner Anfang Januar 2022 die geplante Reform als „große Gefahr“ verdammt, die zu einer „spirituellen Zerstörung“ führen könne. Ein Rabbiner, der sich mit anderen darüber mit dem zuständigen Minister Hendel austauschte, meinte gar: „Aus unserer Sicht ist das schlimmer als der Holocaust. Jemanden zur Sünde zu verleiten, ist schlimmer, als ihn zu töten.“

Die ultraorthodoxen Autoritäten befürchten, von der Regierung ins Abseits gestellt zu werden. Seit langer Zeit sind in der seit Juni 2021 regierenden Koalition erstmals keine religiösen Parteien vertreten, und auch in anderen Bereichen – bei der Konversion zum Judentum oder bei der Zuständigkeit für Koscher-Zertifikate – sind bereits Reformen auf den Weg gebracht worden. Die Rabbiner sind in Sachen Internet aber längst auf verlorenem Posten: Gemäß einer jüngst veröffentlichten Studie sind bereits zwei Drittel aller Ultraorthodoxen in Israel online. Knapp die Hälfte davon nutzt dafür ein Handy. Manch einer nämlich besitzt zwei davon: eins zum Vorzeigen, eins zum Surfen (Münch, Surfen verboten, SZ 09.01.2022, 1).

Israel

Militär erstellt und nutzt Palästinenser-Bilddatenbank

Das israelische Militär hat Bewohner des Westjordanlandes offenbar systematisch fotografieren lassen, um eine Bilderdatenbank zu erstellen. Ex-Soldaten berichteten, die Datenbank mit dem internen Namen „Blauer Wolf“ diene der Feststellung der Identität von Palästinensern, ohne dass diese sich ausweisen. Dafür glichen Sicherheitskameras ihre Aufnahmen mit der Datenbank ab. Wurde ein Palästinenser erkannt, der zur Fahndung ausgeschrieben war, bekamen Soldaten eine Benachrichtigung. Die Armee wollte die Nutzung des Überwachungsprogramms weder bestätigen noch dementieren. Man führe im Rahmen der Terrorismusbekämpfung „Routine-Sicherheitsoperationen“ durch. Die betroffenen Palästinenser beklagen eine immer stärkere Überwachung und den Verlust ihrer Privatsphäre.

Ein Bewohner der 215.000-Einwohner-Stadt Hebron im Westjordanland erklärte, er lasse seine Kinder nicht mehr vor der Tür spielen, um sie dem Blick der vielen Sicherheitskameras zu entziehen. Hebron ist geteilt – ein Teil wird von Israel kontrolliert, der andere von der palästinensischen Autonomiebehörde. Seit Jahrzehnten gibt es Spannungen, weshalb Hebron besonders observiert wird. Die ehemaligen Armeeangehörigen, die das Überwachungsprogramm publik machten, hatten sich zuerst an die Organisation „Breaking the Silence“ gewandt. Die Gruppe besteht aus Ex-Militärs, die sich dafür einsetzen, dass Israel das Westjordanland aufgibt, das seit Jahrzehnten teilweise besetzt ist („Facebook für Palästinenser“, Der Spiegel Nr. 46 13.11.2021, 81).

Saudi-Arabien

Öffentlicher Pranger als Strafe wegen sexueller Belästigung

Yasser Muslim Mohammed al-Arawi ist der erste Mann in Saudi-Arabien, der für die Belästigung einer Frau in Medina öffentlich angeprangert wird. Die saudische Justiz hat in seinem Fall die „Taschhir“-Praxis (öffentliche Anprangerung) angewendet. Al-Arawis kompletter Name, aus dem der Stammbaum abgelesen werden kann, wurde in der lokalen Presse veröffentlicht. In einem Land wie Saudi-Arabien, das sich gesellschaftlich immer noch sehr stark an Stämmen und Abstammungslinien orientiert, ist das eine große Schande und hat dementsprechend, so hoffen wohl die Behörden, auch ein großes Abschreckungspotenzial.

Der Mann, so die Anklage, habe sich der Frau von hinten genähert, sie begrapscht und mit obszönen Worten verfolgt. Ihm drohen nun eine Geldstrafe von umgerechnet rund 1.200 € sowie acht Monate Haft. Seit 2018 wird sexuelle Belästigung in dem konservativen Golfkönigreich mit bis zu zwei Jahren Gefängnis und Geldstrafen von bis zu 24.000 € geahndet. Bei Wiederholungstätern sieht das saudische Strafgesetz sogar eine Haftstrafe von bis zu fünf Jahren vor. Auch einige arabische Länder, darunter Ägypten und Libanon, verschärften kürzlich ihre Gesetze gegen sexuelle Belästigung. Aktivisten beklagen häufig, dass die Gesetze an der laschen Polizeiarbeit scheitern.

Viele reagierten nun erfreut auf die erstmals zur Anwendung gekommene Taschhir-Praxis, die Saudi-Arabien 2021 gesetzlich verankerte. Die Richter des Strafgerichts in Medina, der zweitwichtigsten heiligen Stadt des Islam, griffen anlässlich der „Schwere des Verbrechens und seiner Auswirkungen auf die Gesellschaft“, wie es im Gesetzestext steht, darauf zurück. Besonders erniedrigend dabei ist, dass der Täter die Zeitungen auch noch dafür bezahlen muss seinen Namen abzudrucken.

In der arabischen Öffentlichkeit ist in den vergangenen Jahren eine höhere Sensibilität bei dem Thema sexuelle Belästigung zu beobachten. Während einige zwar immer noch über die Kleidung der Frau diskutieren wollen, anstatt die Schuld alleine bei dem Täter zu suchen scheint sich die Mehrheit einer Nulltoleranz-Haltung anzunähern. Der saudische Anwalt Khalid Abu Rashid bezeichnete im Live-Fernsehen des Senders Rotana al-Khalijia schon die Frage nach der Handynummer oder dem Snapchat-Namen als Beginn einer möglichen Belästigung: „Es beginnt mit einem Wort.“ Frauen – oder auch Männer – sollten in diesem Fall Zeugen auf die Situation aufmerksam machen oder sich nach Überwachungskameras umsehen.

In den sozialen Netzwerken wurde das Urteil größtenteils positiv aufgenommen. Es gab aber auch kritische Stimmen, vor allem von männlichen Usern. Nun sei der Name einer ganzen Großfamilie in den Schmutz gezogen, dabei träfe sie doch keine Schuld, schrieb einer. Die Antwort von weiblicher Seite folgte

sogleich: Die Großfamilie sei schuld, weil sie den Abkömmling offensichtlich nicht richtig erzogen habe. Außerdem fordern viele Frauen neben der Veröffentlichung des Namens auch ein Foto des Täters, es könne ja sonst zu Verwechslungen kommen. Einige forderten sogar den Wohnort des Täters, sie würden ihn gerne besuchen (Ramadan, Der Name in der Zeitung, SZ 13.01.2022, 6).

Russland

Daten von einer halben Million Impfbetrügern zum Verkauf

Die personenbezogenen Daten von 500.000 Menschen aus Moskau und Umgebung werden im Darknet und auf Telegram-Kanälen zum Kauf angeboten. Die Datensätze beinhalten Ausweisdaten, Sozialversicherungsnummern, Telefonnummern und Adresse. Zuvor hatten sich, so Presseberichte, alle in den Datensätzen befindlichen Personen ein gefälschtes Impfzertifikat beziehungsweise einen gefälschten PCR-Test ausstellen lassen.

Evgeny A., Programmierer und Betreiber eines Telegram-Kanals für Leaks von Daten im russischen Internet mit dem Namen „Eye of God“, erklärte, dass die größte Datenbank mehr als 500.000 Einträge über Bewohner aus Moskau enthält. Ihm zufolge wurden die Daten vom gleichen Dienst geleakt, der den Moskauern auch die gefälschten Corona-Zertifikate verkaufte.

Für die Daten einer einzelnen Person, die auch das Ausstellungsdatum des gefälschten Zertifikats enthält, werden dem Bericht nach umgerechnet etwa 40 Euro-Cents aufgerufen. Der Zeitung Kommersant, die Kontakt zu einem Anbieter der Daten aufgenommen hatte, wurden 1.000 Datensätze für umgerechnet 104 Euro angeboten.

Einem Rechtsexperten zufolge drohen bei Erwerb eines gefälschten Impfzertifikates und dessen Ausstellung auch strafrechtliche Konsequenzen – bis zu einem Jahr Haft für den Erwerb, für die Erstellung gefälschter Impfzertifikate sogar bis zu zwei Jahre. Ein Darknet-Experte vermutet, dass die Betrüger wahrscheinlich doppelt abkassieren wollen (Mewes, Daten von 500.000 Moskauern mit gefälschten Impfzertifikaten stehen zum Verkauf, www.heise.de 14.11.2021, Kurzlink: https://heise.de/-6266421).

USA

NSO wegen Pegasus sanktioniert

Das US-Handelsministerium hat unter anderem zwei israelische Softwareanbieter auf die Liste der Unternehmen gesetzt, die Handelsbeschränkungen unterliegen. Betroffen sind die Entwicklerfirma der berüchtigten Spionagesoftware Pegasus NSO sowie eine Softwarefirma namens Candiru. Sie gelangten auf die „Entity List“, weil es Beweise gebe, dass sie „Spionagesoftware entwickelt und an ausländische Regierungen geliefert haben“. Die Software sei zur „Überwachung von Regierungsbeamten, Journalisten, Geschäftsleuten, Aktivisten, Wissenschaftlern und Botschaftsmitarbeitern eingesetzt“ worden.

Die NSO Group war mit ihrer Spionagesoftware Pegasus im Sommer 2021 weltweit in die Schlagzeilen geraten, nachdem bekannt wurde, dass Staats- und Regierungschefs sowie mindestens 180 Journalisten, Menschenrechtsverteidiger, Wissenschaftler, Gewerkschafter und Diplomaten mit der Software ausspioniert wurden. NSO wird darüber hinaus vorgeworfen seine Software regelmäßig an autoritäre Regierungen zu verkaufen, die damit Journalisten und die Opposition überwachen. Das Unternehmen weist die Vorwürfe ebenso regelmäßig zurück (DANA 3/2021, 187 ff.). Auch die Bundesregierung gehört zu den Kunden der NSO Group; das BKA hat Pegasus eingekauft (DANA 4/2021, 239 f.).

Candiru ist ein israelisches Unternehmen, das im Sommer mit Exploits für Zero-Day-Lücken in beliebten Browsern aufgefallen war. Der Firma werden Spyware-Tools für verschiedene Plattformen wie iOS, Android, Windows oder MacOS zugeschrieben, darunter ein Tool namens DevilsTongue. Microsofts Threat Intelligence Center (MSTIC) hatte zuletzt über 100 Ziele der Spyware beobachtet.

Neben den zwei israelischen Spyware-Schmieden landeten auch das russische Unternehmen Positive Technologies und die Computer Security Initiative Consultancy aus Singapur auf der Entity List. Die US-Regierung geht davon aus, dass diese Firmen mit Software handeln, „die dazu dienen, sich unbefugt Zugang zu Informationssystemen zu verschaffen und damit die Privatsphäre und Sicherheit von Einzelpersonen und Organisationen weltweit bedrohen“. Auf der Entity List führt die US-Regierung Unternehmen, Personen oder Regierungen, deren Aktivitäten „den nationalen Sicherheits- oder außenpolitischen Interessen der Vereinigten Staaten zuwiderlaufen“. Der Handel mit diesen unterliegt strengen Beschränkungen und ist teilweise nur mit einer Ausnahmegenehmigung des Ministeriums erlaubt.

Im Mai 2019 hatte die US-Regierung unter Präsident Donald Trump auch Huawei auf diese Liste gesetzt. Das hatte weitreichende Folgen für das chinesische Unternehmen und seine zahlreichen US-Handelspartner. Huawei kann wegen der Beschränkungen unter anderem keine Smartphones mit Googles Android mehr anbieten und hatte sich dann von einem großen Teil seines Smartphone-Geschäfts getrennt (Strafe für Pegasus-Firma NSO, SZ 04.11.2021, 20; Briegleb, Spyware Pegasus: USA verhängen Sanktionen gegen NSO Group und andere, www.heise.de 03.11.2021, Kurzlink: https://heise.de/-6250364).

USA

Apple klagte gegen NSO wegen Pegasus

Am 23.11.2021 reichte Apple vor einem US-Bundesgericht Klage gegen NSO ein. Die NSO Group aus Israel ist für ihre Software Pegasus bekannt. Mit Pegasus übernehmen NSO-Kunden, meist Polizeien und Geheimdienste, aus der Ferne Handys. Sie können auf praktisch alle Daten des Geräts zugreifen, es als Wanze benutzen und sogar die Kamera an- und ausschalten. Damit soll nun zumindest in Bezug auf iPhones Schluss sein. Apple will Schadenersatz in ungenannter Höhe und dem Unternehmen verbieten Apples Geräte und

Dienste zu nutzen. Das soll laut Apple „weiteren Missbrauch und Schaden bei Nutzern verhindern“. Apple begründet seine Klage damit, dass diejenigen, die Pegasus einsetzen, gegen Apples Nutzungsbestimmungen verstoßen, wenn sie sich Apple-Konten anlegen, um andere auszuhorchen. NSO erklärte dazu nur allgemein: „Pädophile und Terroristen operieren frei in technologischen Schutzzonen, und wir geben Regierungen die legalen Mittel dagegen zu kämpfen.“ Apple erklärte, die NSO Group müsse für „die Überwachung von und den gezielten Angriff auf Apple-Nutzer“ zur Verantwortung gezogen werden. Das Unternehmen beantragte darüber hinaus eine dauerhafte Verfügung, „die der NSO Group die Nutzung jeglicher Software, Services oder Geräte von Apple untersagt“.

NSO wird vorgeworfen ihre Software auch an Regierungen zu verkaufen, die sie gegen demokratische Oppositionelle und andere missliebige Politiker einsetzen statt nur gegen Verbrecher und Terroristen, wie das Unternehmen behauptet. Im Sommer hatten Enthüllungen eines internationalen Konsortiums von Journalisten gezeigt, wie Pegasus mutmaßlich missbraucht worden ist: Hunderte Menschenrechtsaktivisten, Journalisten, Anwälte und Staatschefs wurden offensichtlich ausspioniert. NSO bestreitet die Vorwürfe und verweist auf Vorgaben für seine Kunden, die Menschenrechte einzuhalten (DANA 3/2021, 187ff., s.o. S. 49).

Unternehmen wie Apple sind in der digitalen Spionagewelt in einer besonderen Position. Ihre Infrastruktur – in diesem Fall das Betriebssystem des iPhone – ist der Kanal, über den Spione sich Zugriff auf die Geheimnisse ihrer Ziele verschaffen. Fachleute nennen die Angriffstechnik, mit der NSO mutmaßlich in iPhones eindringt „Forcedentry“ – gewaltsames Eindringen.

Apples Software-Chef Craig Federigh erklärte: „Staatlich geförderte Akteure wie die NSO Group geben Millionen von US-Dollar für ausgeklügelte Überwachungstechnologien aus, ohne dass eine wirksame Rechenschaftspflicht besteht. Das muss sich ändern“. Apple betont zugleich, dass die „ausgeklügelte, staatlich geförderte Überwachungstechnologie“ nur auf „eine sehr geringe Anzahl von Nutzern“ abziele und nicht nur iOS betreffe, sondern auch Googles Android.

Apple will zudem die NGOs Citizen Lab, eine Forschungsgruppe an der Universität Toronto, und Amnesty Tech mit zehn Millionen Dollar unterstützen. Die Organisationen untersuchen von der Pegasus-Software befallene Handys forensisch und rekonstruieren so Spionageaktionen. Das Citizen Lab soll außerdem mit kostenloser Technik und mit technischer Hilfe unterstützt werden. Apple schlägt sich damit klar auf die Seite jener nicht-kommerziellen IT-Fachleute, die Dissidenten vor Überwachung schützen wollen. Das Geld, das Apple von NSO erstreiten will, möchte der Konzern an die beiden Unternehmen spenden. Ron Deibert vom Citizen Lab lobte das Vorgehen von Apple. Er hoffe, Apple werde Gerechtigkeit für alle „Opfer des rücksichtslosen NSO-Verhaltens“ herstellen.

iPhones haben bzgl. ihrer Sicherheit einen guten Ruf. Umso peinlicher ist es für das Unternehmen, dass NSO Schwachstellen ausnutzen konnte. Apples IT-Sicherheitsabteilung hatte die Schwachstellen, die Pegasus ausnutzte, nicht selbst entdeckt und geschlossen. Apple versucht somit einmal mehr sich als jener Tech-Konzern zu profilieren, der sich dem weltweiten System digitaler Überwachung nicht nur verweigert, sondern es sogar aktiv bekämpft. Für Apple ist das einfacher als für Konzerne wie Facebook oder Google: Die Kalifornier verdienen ihr Geld vor allem mit dem Verkauf von Hardware und weniger mit Werbung.

Apple kündigte zudem an Nutzende direkt zu informieren, wenn der iPhone-Hersteller davon ausgeht, dass sie Opfer einer solchen Spionagekampagne wurden. So soll es künftig sogenannte Threat Notifications über die zentrale Nutzerverwaltungsseite des Konzerns, per E-Mail sowie falls möglich auch per iMessage geben. Wie genau Apple solche Angriffe erkennen will, um seine Nutzer zu informieren, ist unklar.

Apple ist der zweite Konzern aus dem Silicon Valley, den sich die NSO Group zum Feind macht. Meta (ehemals: Facebook) klagt schon seit 2019 gegen NSO, weil Whatsapp-Nutzende mit Pegasus angegriffen worden sein sollen. Anfang November 2021 scheiterte NSO vor einem US-Gericht mit dem Argument, man genieße Immunität, weil man ja im Auftrag ausländischer Regierungen gehandelt habe. Die USA haben NSO mittlerweile auf ihre Sanktionsliste gesetzt (s. S. 53). US-Unternehmen dürfen der Firma keine Technologie mehr verkaufen (Brühl, Runter von meinem Grundstück, SZ 25.11.2021, 19; Grünewald, Apple geht gegen Spyware vor, www.heise.de 24.11.2021, Kurzlink: https://heise.de/-6275628; Briegleb, Spyware Pegasus: Apple verklagt NSO Group, www.heise.de 23.11.2021, Kurzlink: https://heise.de/-6275153).

USA

Familie klagt auf Entschädigung wegen Patenterlösen

70 Jahre nach dem Tod von Henrietta Lacks verklagte die Lacks-Familie am 04.10.2021 mehrere Pharmafirmen. 1951 wurden der Afro-Amerikanerin im John Hopkins-Krankenhaus ohne ihr Einverständnis Krebszellen entnommen. Am 04.10.1951 starb sie an Gebärmutterkrebs. Die „Hela“-Zellen sind die ersten Zellen, die im Labor vermehrt werden konnten. Sie revolutionierten die medizinische Forschung und führten zu Medikamenten, Impfungen und neuen Technologien. Inzwischen sind mehr als 17.000 Patente dokumentiert, die mit den Hela-Zellen in Verbindung stehen. Die verklagten Unternehmen haben mit diesen Zellen Millionen US-Dollar Profite gemacht, wovon die Familie keinen Cent erhielt. Diese verlangt eine finanzielle Entschädigung sowie einen Verzicht der Forschung auf Hela-Zellen ohne ihr Einverständnis (GiD Nr. 259 November 2021, 28 f.).

Kanada

Datenschutzbehörden gehen gegen Clearview-Gesichtsbilderdienst vor

Der biometrische Gesichtserkennungsdienst Clearview AI muss alle Bilder und Gesichtsdaten von Einwohnern

der kanadischen Provinzen Québec, Alberta und Britisch-Kolumbien löschen. Außerdem darf Clearview seinen Gesichtserkennungsdienst dort auf Dauer nicht mehr anbieten. Das haben die Datenschutzbehörden der drei Provinzen entschieden. Clearview vertritt den Standpunkt, die Bilder und Gesichtsdaten könnten gar nicht gelöscht werden.

Mehr als drei Milliarden Gesichtsfotos hat das New Yorker Unternehmen Clearview AI im Internet zusammengesucht. Damit hat es einen Gesichtserkennungs-Algorithmus trainiert, den es vermietet. Die Firma hat erst gar nicht versucht die Zustimmung der Betroffenen einzuholen. Daraufhin haben Google, LinkedIn, Meta, Twitter und YouTube den Fotosammler mit Unterlassungsaufforderungen eingedeckt, weil das Abgreifen der Nutzerbilder gegen die Nutzungsbestimmungen der jeweiligen Dienste verstößt.

Im Februar 2021 hat die kanadische Datenschutzbehörde offiziell festgestellt, dass Clearview AI mehrfach gegen kanadisches Bundesrecht verstoßen hat und Clearviews Gesichtserkennungsdienst illegal ist. Die Behörden Australiens und Großbritanniens haben ähnliche Feststellungen getroffen. Das Unternehmen hat seinen Dienst zwar für kanadische Kunden pausiert, möchte den Betrieb aber wieder aufnehmen. Dazu verlangt es, dass die Behörden Richtlinien ausarbeiten, die den legalen Betrieb in Kanada ermöglichen. Darüber hinaus begehrte Clearview vergeblich die Geheimhaltung des kanadischen Behördenberichts.

Weil sich die Firma weiterhin keiner Schuld bewusst ist, weiter Gesichtsfotos sammeln möchte, die bereits gesammelten Bilder nicht gelöscht hat und die kanadischen Behörden als unzuständig erachtet, haben nun drei Provinzen rechtlich verbindliche Bescheide erlassen (Alberta Order P2021-12, Umsetzung binnen 90 Tagen, Britisch-Kolumbien Order P21-08, Umsetzung binnen sechs Wochen, Québec Dossier 1023158-S, Umsetzung binnen 90 Tagen). Clearview hatte in den Verfahren erneut die Anwendbarkeit kanadischen Rechts sowie die Zuständigkeit der dortigen Behörden in Abrede gestellt.

Außerdem behauptet Clearview, es sei unmöglich die einschlägigen Bilder zu löschen. Aus den Bildern ginge nicht hervor, wo sie aufgenommen wurden. Gleichzeitig verspricht das Unternehmen seinen Kunden die gezeigten Personen identifizieren zu können. Dann müsste sich ja auch feststellen lassen, wo diese Personen leben. Clearview hatte sich in einem Verfahren im US-Staat Illinois ganz anders geäußert: Dort hat es alle Bilder, deren Metadaten einen Aufnahmeort in Illinois verraten, von der Suche ausgeschlossen. Es sammelt auch keine Bilder mehr von Servern, die Illinois zugeordnete IP-Adressen haben, oder in deren URL Stichworte wie Illinois oder Chicago vorkommen. Zudem hat Clearview für Einwohner Illinois' ein Opt-Out-Verfahren eingerichtet. Daher schenken Kanadas Datenschutzbehörden den Behauptungen Clearviews, nichts unternehmen zu können, keinen Glauben.

Während Clearview AI in Großbritannien eine Millionenstrafe droht, können Kanadas Datenschutzbehörden erst dann Strafen verhängen, wenn den nun ausgestellten Bescheiden nicht Folge geleistet wird. Und selbst dann sind die maximalen Strafhöhen in Alberta und Britisch-Kolumbien mit 100.000 kanadischen Dollar (knapp 69.000 Euro) gering. Allerdings könnten Betroffene Schadenersatz verlangen (Sokolov, Kanadische Behörden verbieten Clearviews Gesichtserkennung, www.heise.de 16.12.2021, Kurzlink: https://heise.de/-6296459; s.o. S. 45).

El Salvador

Pegasus-Spähsoftware auf Handys von Regierungskritikern

Auch nach Beginn der jüngsten Enthüllungen rund um die israelische NSO Group im vergangenen Sommer (DANA 4/2021, 187 ff.) wurden gemäß einer gemeinsamen Recherche des kanadischen Citizen Lab mit Bürgerrechtsorganisationen Journalisten und Aktivisten in El Salvador mit NSO-Spyware ausgespäht. Erfolgreiche Spyware-Angriffe fanden demnach zwischen Juli 2020 und November 2021 statt. Die Analyse sei begonnen worden, nachdem Journalisten und Journalistinnen aus dem mittelamerikanischen Staat mit einem Werkzeug von Amnesty International auf ihren Smartphones Hinweise auf die Pegasus-Malware gefunden hatten. Gezielte Nachforschungen ergaben, dass vor allem Angestellte der Nachrichtenseite El Faro aus San Salvador betroffen waren, aber auch solche anderer Medien und zivilgesellschaftlicher Organisationen.

In den Monaten nach den ersten Enthüllungen ist die Liste der von der Pegasus-Ausspähung Betroffenen immer länger geworden. Von immer mehr Staaten wurde bekannt, dass sie die Spyware erworben hatten. Die NSO Group hatte die damit verbundenen Vorwürfe zurückgewiesen und versichert nur mit legitimen, vom israelischen Verteidigungsministerium überprüften Regierungsstellen zusammenzuarbeiten.

In El Salvador wurde die Spyware nun auf den Mobiltelefonen von 37 Personen gefunden, 23 davon arbeiten für El Faro, vier für das Magazin GatoEncerrado. Beide Publikationen haben auch Berichte publiziert, in denen Kritik an der Regierung geübt wurde. Präsident von El Salvador ist seit 2019 Nayib Bukele, der Bitcoin zum offiziellen Zahlungsmittel seines Landes gemacht hat und wiederholt die Medien attackiert und zu „Feinden des Volkes" erklärt. Auf dem Index der Pressefreiheit von Reporter ohne Grenzen rutschte El Salvador zuletzt um acht Plätze auf Rang 82 ab. Das Citizen Lab beschuldigt nun niemanden namentlich die Spyware-Angriffe in Auftrag gegeben zu haben, weist aber darauf hin, dass die Fälle in „bedrückender Weise mit den Interessen der Regierung Bukele übereinstimmen" (Holland, NSO: Pegasus-Spyware auch bei Dutzenden Journalisten in El Salvador gefunden, www.heise.de 13.01.2022, Kurzlink: https://heise.de/-6325951).

Iran/China

Iran beschafft chinesische Überwachungstechnik

Laut einem neuen Bericht der in den USA ansässigen Forschungsgruppe für Überwachungssysteme IPVM verkauft das chinesische Unternehmen Tiandy seine Überwachungstechnologie an die

Revolutionsgarde, die Polizei und das Militär im Iran. Die Firma ist eines der größten Videoüberwachungsunternehmen der Welt mit einem Umsatz von fast 700 Mio. US-Dollar im Jahr 2020. Sie handelt mit Kameras und dazugehöriger KI-gestützter Software, darunter Gesichtserkennungstechnologie und einer Software, die angeblich die Rasse einer Person erkennen kann. Auch im Portfolio: „intelligente" Vernehmungstische, die zusammen mit „Tigerstühlen" verwendet werden können. An diesen Stahlstühlen werden Gefangene zur Folter in schmerzhaften Körperhaltungen stundenlang fixiert.

Gemäß dem IPVM-Bericht setzt die chinesische Regierung Tiandys „Ethnicity Tracking"-Tool zur Unterdrückung der uigurischen Minderheit in der Provinz Xinjiang ein, eines von mehreren KI-basierten Systemen, das Experten weithin als ungenau und unethisch bewerten. Der IPVM-Bericht beruht auf einer Analyse öffentlich zugänglicher Social-Media-Posts und Tiandys Werbung im Netz. Daraus geht hervor, dass das Unternehmen einen Fünfjahresvertrag im Iran unterzeichnet hat und dort angeblich acht einheimische Mitarbeiter beschäftigt. Tiandy ist zwar in Privatbesitz, aber ein wichtiger Lieferant der chinesischen Regierung und sein CEO, Dai Lin, ein öffentlicher Unterstützer der Kommunistischen Partei. Welche Überwachungsmöglichkeiten Tiandy genau an den Iran verkauft, ist unklar. IPVM fand Tiandy-Kameras im Einsatz bei der iranischen Firma Sairan – einem „staatlichen Anbieter von Militärelektronik" – und in einer geheimen Militärbasis. Tiandy wirbt auf seiner öffentlichen Website auch mit mehreren Projekten im Iran, darunter die Zusammenarbeit mit der Islamischen Revolutionsgarde und der Polizei in der nördlichen Stadt Khomam.

Das iranische Militär verwendet gemäß IPVM vernetzte Videorekorder (NVR) von Tiandy, die mit Chips des US-Herstellers Intel betrieben werden. Daher stellt sich die Frage, ob das Unternehmen gegen die US-Sanktionen gegen den Iran verstößt. Penny Bruce, eine Sprecherin von Intel, erklärte: „Wir wissen nichts über die Hintergründe der erhobenen Vorwürfe und untersuchen die Situation."

Experten vermuten schon lange, dass der Iran versucht ein System der digitalen Kontrolle über seine Bürger nach dem Vorbild Chinas und unter Verwendung chinesischer Werkzeuge auszubauen. Saeid Golkar, Experte für iranische Sicherheit an der University of Tennessee, Chattanooga, sagte, dass Zensur und Überwachung die Grundpfeiler dieses Modells seien: „Die Islamische Republik versucht ein Internet nach chinesischem Vorbild zu schaffen, indem sie eine starke Vernetzung fördert und dann kontrolliert."

Der Iran hat schon früh das chinesische „Social Credit"-System übernommen, eine umfassende Erfassung und Analyse (Scoring) der finanziellen, bürgerlichen und sozialen Aktivitäten der Bürger. Im Jahr 2010 unterzeichnete das in Shenzhen ansässige Unternehmen ZTE ein 130-Millionen-Dollar-Geschäft mit der staatlichen Telecommunication Company of Iran (TCI), die ein Überwachungssystem in die von der Regierung verwaltete Telefon- und Internetinfrastruktur integrierte.

Im März 2021 vereinbarten China und der Iran eine strategische Partnerschaft mit einer Laufzeit von 25 Jahren. Viele Details sind nicht bekannt, wohl aber, dass das Abkommen eine verstärkte militärische und handelspolitische Zusammenarbeit zwischen den beiden Ländern vorsieht. Der IPVM-Bericht zeigt bestätigend auf, wie der Iran seine Überwachungsmethoden modernisiert. Golkar zufolge wurde der iranische Sicherheitsapparat bis vor kurzem größtenteils von Moderatoren und Informanten geleitet, die Websites in den sozialen Medien überwachten. Das ändere sich gerade rapide: „Mit der zunehmenden Digitalisierung des Irans werden wir sicher auch mehr digitale Formen der Unterdrückung und Überwachung erleben." Der Iran ist bekannt für die Inhaftierung und Folterung von Dissidenten, und die Produktlinie von Tiandy scheint gut geeignet zu sein solche Methoden zu unterstützen.

Golkar betont, dass es wichtig ist zu beobachten, was China anderen Ländern und insbesondere Autokratien zu verkaufen versucht, die China folgen: „Alles, was China macht, werden sie kaufen oder versuchen es zu kopieren". Die Partnerschaft zwischen Tiandy und dem Iran ist ein Beleg des besorgniserregenden Trends (Ryan-Mosley, Chinesisches Unternehmen verkauft Videoüberwachungssysteme an Iran, www.heise.de 20.12.2021, Kurzlink: https://heise.de/-6297914).

Technik-Nachrichten

Facebook schaltet Gesichtserkennung ab

Nachdem die 2010 eingeführte Gesichtserkennung von Facebook jahrelang für Kritik von Datenschützern, insbesondere aus Europa, gesorgt hat, kündigte der Facebook-Betreiber Meta Anfang November 2021 an sein Gesichtserkennungssystem abzuschalten. Mit der Funktion konnten Nutzer automatisch in Fotos markiert werden. Ganz aufgeben will der Konzern die Technologie aber nicht. Jerome Pesenti, Vizepräsident für künstliche Intelligenz bei der neuen Facebook-Muttergesellschaft Meta erklärte, die gespeicherten Gesichtsdaten von mehr als einer Milliarde Menschen würden gelöscht: „Diese Änderung wird eine der größten Veränderungen in der Nutzung der Gesichtserkennung in der Geschichte der Technologie darstellen." Das System ist bisher eines der größten digitalen Fotoarchive der Welt. Mehr als ein Drittel der täglich aktiven Facebook-Nutzer habe sich für die Gesichtserkennungseinstellung entschieden, rechnete er in einem Blogbeitrag vor. Das entspricht rund 640 Millionen Menschen. Zuletzt mussten die Nutzenden ausdrücklich zustimmen, damit ihre Namen in Fotos den Facebook-Freunden automatisch angezeigt wurden.

Weil die Technologie in den vergangenen Jahren aber stetig besser wurde, steht sie immer mehr in der Kritik. So setzt die chinesische Regierung Gesichtserkennungssoftware ein, z.B. um die muslimische Minderheit der Uiguren zu überwachen. Polizeibehörden in den USA nutzen die Technik ebenfalls. In einigen Bundesstaaten und Städten ist sie aber mittlerweile wieder verboten worden, um Missbrauch zu verhindern.

Relativierend meinte Pesenti, das Unternehmen versuche, die positiven Anwendungsfälle für die Technologie „gegen die wachsenden gesellschaftlichen Bedenken abzuwägen, zumal die Regulierungsbehörden noch keine klaren Regeln aufgestellt haben". Man sehe „eine Reihe von Fällen, in denen die Gesichtserkennung von hohem Wert für die Nutzer der Plattform sein kann" (Facebook stellt umstrittene Gesichtserkennung ein, www.spiegel.de 02.11.2021; Schuler, Facebook schaltet Gesichtserkennung ab, www.tagesschau.de 03.11.2021; Ohne Gesichtserkennung, SZ 04.11.2021, 20).

Meta-Ankündigung: Kein Targeting mit sensiblen Merkmalen

Meta – wie das Unternehmen hinter Facebook, Instagram und Whatsapp seit Kurzem heißt – will Werbetargeting diskriminierungsfreier machen. Von Januar 2022 an sollen Werbetreibende keine Zielgruppen mehr auswählen können, die Nutzer nach ihrem Gesundheitsstatus, ihrer politischen, religiösen oder sexuellen Orientierung unterteilen. Solche Informationen leiten die Systeme von Meta automatisch daraus ab, mit welchen Inhalten die Nutzer sich beschäftigen. Eine Anzeige, die nur Frauen zwischen 25 und 35 Jahren zu sehen bekommen, würde also weiterhin online gehen können, aber keine Anzeige nur für lesbische Kommunistinnen dieses Alters.

Menschen berichten immer wieder, wie eingeengt sie sich auf bestimmte intime Merkmale durch Anzeigen-Targeting fühlen. Wer z.B. kürzlich einen Trauerfall in der Familie hatte bekommt massenweise Grabsteine zu sehen. Zumindest „sensible" persönliche Informationen sollen künftig aus dem eigenen Werbeprofil ausgeklammert bleiben.

Die Werbetreibenden müssen also eventuell auf ein breiter angelegtes Targeting zurückgreifen und somit auf Facebooks sogenanntes Auslieferungssystem. Je weniger detailliert die Nutzer selbst das Targeting auswählen, desto stärker ermittelt dieses System mithilfe künstlicher Intelligenz automatisch, welche Menschen wohl am empfänglichsten sind für welche Anzeigen. Dabei passiert das, was immer passiert, wenn man dem KI-System derlei Entscheidungen überlässt: Sie verstärken bestehende Stereotype. Die Organisation Algorithm Watch hat in einem Versuch gezeigt, dass Facebook Jobangebote für Lastwagenfahrer viel häufiger Männern zeigt, Anzeigen für Kindererzieher hingegen eher Frauen. Die Werbetreibenden diskriminieren künftig also eventuell weniger selbst. Sie lassen vollautomatisch diskriminieren.

Politische Organisationen befürchten, dass die geplanten Änderungen ihre Arbeit erschweren könnten. Die Organisation Campact etwa gibt an Facebooks Werbesystem zu nutzen, um Menschen über ihre Interessen an bestimmte Themen auf laufende Kampagnen hinzuweisen, etwa zu „Fridays for Future" oder „Christopher Street Day". Beides dürfte künftig in die Kategorie dessen fallen, was Facebook als politisch und insofern als „sensibel" einzustufen gedenkt. Die Organisation Transgender Europe teilt mit, sie bitte Facebook dringend „sicherzustellen, dass LGBTIQ-Aktivisten und -Organisationen eine Möglichkeit haben sich an ihre Mitglieder und Gemeinschaft zu wenden". Das Kürzel LGBTIQ steht für sexuelle Minderheiten.

Meta erklärt: „Wir wissen, dass diese Änderung negative Auswirkungen auf einige Unternehmen und Organisationen haben könnte." Man habe sich die Entscheidung nicht leicht gemacht. Trotzdem kann der Konzern sich nun rühmen etwas im Kampf gegen die Diskriminierung und das bei vielen Menschen verhasste Targeting zu tun. Nach den jüngsten Enthüllungen skrupelloser Geschäftspraktiken durch die Whistleblowerin Frances Haugen hat Meta bzw. Facebook eine besonders offene Flanke. Ein Gesetz über digitale Dienste der EU, das die Möglichkeiten „personalisierter Werbung" einschränken soll, befindet sich auf der Zielgeraden (Bovermann, Facebook dreht am Anzeigen-Algorithmus, SZ 11.11.2021, S. 6).

Verräterische Fingerschweiß-Analyse

Ein Team um den Chemiker Christopher Gerner von der Universität Wien hat demonstriert, dass winzige Schweißtöpfchen an der Unterseite der Fingerkuppen viel über Verhalten und Gewohnheiten einer Person preisgeben. In der Zeitschrift „Nature Communications" berichten sie, dass das an den Fingerspritzen abgesonderte Sekret zwar zu 99% aus Wasser besteht, dass darin aber auch jede Menge Elektrolyte sowie Harnstoff, Laktat, Aminosäuren, Metall-Ionen, diverse Stoffwechsel-Abbauprodukte und körperfremde Substanzen, deren Zusammensetzung sich je nach Person unterscheidet, zu finden sind. Die Forschenden konnten bisher 250 Substanzen mit ihrer neuen Methode schneller und einfacher nachweisen als etwa mit der sonst üblichen Urin- oder Blutanalyse.

Danach genügen wenige Millionstel Milliliter Schweiß am Finger, um zu erfahren, was chemisch im Körper passiert ist. Wie stumme Zeugen liefern die Substanzen Hinweise, wie lange der letzte Espresso her ist, ob kürzlich Kokain, Ecstasy oder Cannabis konsumiert wurden, ob jemand die Antibabypille, Psychopharmaka oder Betablocker nimmt oder ob eine zuvor gegessene Bio-Orange besonders viele Antioxidantien enthalten hat. Gemäß Gerner ist deren Methode unkompliziert, da man nur eine Minute lang ein spezielles Filterpapier zwischen Daumen und Zeigefinger halten müsse. Die im Schweiß vorkommenden Moleküle werden anschließend im Labor extrahiert und per Massenspektrometer analysiert. Sind die enthaltenen Substanzen bereits bekannt, dauert dies nur etwas mehr als eine Viertelstunde.

Für ihre Studie hat das Team die Testpersonen entweder einen Espresso oder Koffeintabletten schlucken lassen. Schon 15 Minuten nach der Einnahme der Koffeinprodukte konnten die For-

schenden in den Fingerabdruck-Proben bereits 35 Inhaltsstoffe und Abbauprodukte nachweisen, darunter Koffein, Theobromin oder Chlorogensäure. Durch weitere Tests zu einem späteren Zeitpunkt ließ sich auch verfolgen, wie sich die Verstoffwechslung des Kaffees und der Tabletten allmählich verändert. Sie konnten u.a. die Hormone Progesteron, Melatonin oder Cortisol sowie den Botenstoff Dopamin aufspüren. Nun suchen die Wissenschaftler nach Anwendungsmöglichkeiten. Ihr Ziel sei es zum Beispiel Stressindikatoren für Herzinfarkt-Risikopatienten rechtzeitig und ohne viel Aufwand zu erkennen. Auch den Laktat-Test für Leistungssportler will das Team vereinfachen. Anstatt dem klassischen Piks ins Ohrläppchen für eine Blutanalyse soll in Zukunft der Fingerschweiß ausreichen, um den Gehalt an Laktat zu bestimmen.

Gerner schätzt, dass sich im Fingerabdruck vermutlich mehrere Tausend Stoffe nachweisen lassen: „Bei einigen Testpersonen haben wir jetzt zum Beispiel Hinweise auf Dutzende Pestizide im Gemüse gefunden oder bei Rauchern diverse Substanzen aus dem Zigarettenrauch.“ Die Forensik sei an der neuen Analysetechnik sehr interessiert. Fachleute von der Abteilung Forensische Medizin der Universität Wien überprüfen, ob die Methode auch bei zu untersuchenden Leichen noch Hinweise auf den Konsum möglicher Drogen oder Medikamente geben könnte (Reye, Cannabis und Orangen, SZ 25.11.2021, 15).

Rechtsprechung

EGMR

Online-Anonymität bei geschützter Meinungsäußerung

Der Europäische Gerichtshof für Menschenrechte (EGMR) hat am 07.12.2021 einstimmig entschieden, dass Österreich mit nationalen Urteilen zur Herausgabe persönlicher Daten von Nutzern eines Online-Diskussionsforums der Zeitung „Standard“ gegen die in Artikel 10 der Europäischen Menschenrechtskonvention (EMRK) geschützte Meinungsfreiheit verstoßen hat (Nr. 39378/15). Die Straßburger Richter betonten, dass eine Pflicht zur Offenlegung von Informationen über die User „eine abschreckende Wirkung“ auf die öffentliche Debatte habe.

In der Auseinandersetzung ging es um die Preisgabe der Identität von drei Foren-Teilnehmern, deren Beiträge aus den Jahren 2011 bis 2013 unter anderem den österreichischen Rechtspopulisten Herbert Kickl (FPÖ) sowie die Freiheitlichen in Kärnten, eine Landesgruppe der FPÖ, zu Klagen veranlasst hatten. Die Verlagsgesellschaft hatte die Kommentare, in denen rechtsgerichtete Politiker mit Korruption oder Neonazis in Verbindung gebracht wurden, zwar geprüft und entfernt. Sie weigerte sich aber, die persönlichen Daten der Verfasser der Postings preiszugeben.

Ein Online-Artikel von 2012 über das Spitzenpersonal der Kärntner Freiheitlichen führte in dem Forum zu über 1600 Kommentaren. Einer davon lautete: „Korrupte Polit-Arschlöcher vergessen, wir nicht WAHLTAG IST ZAHLTAG!!!!!“ (Wiedergabe wie im Original). Ein anderer Leser machte sich für ein Verbot solcher Rechtsaußenparteien „wegen ihrer dauernden Nazi-wiederbelebung“ stark. Unter einem Interview mit Kickl von 2013, der damals FPÖ-Generalsekretär und inzwischen Chef der Partei ist, beklagte ein Nutzer zudem ein „sägen an der verfassung“ sowie „das destabilisieren unserer staatsform“. Wären solche Taten konsequent unter Strafe gestellt oder zumindest der Mafiaparagraf einmal angewendet worden auf die rechtsextreme Szene in Österreich, gälte Kickl als „einer der größten verbrecher der 2ten republik“.

Der Oberste Gerichtshof (OGH) in Wien urteilte 2014 in letzter Instanz, dass der „Standard“ die Nutzerdaten wegen der Beiträge herausgeben muss. Die Verlagsgruppe legte daraufhin 2015 Beschwerde beim EGMR ein. Sie argumentierte, die Kommentare seien zulässige kritische Werturteile im politischen Zusammenhang. Es handle sich nicht um einen rechtlich unzulässigen „Wertungsexzess“. Die Beiträge basierten in wesentlichen Punkten auf nachweisbaren Tatsachen. Das Urteil zur Preisgabe der Identitäten verletze nicht nur die Meinungs- und Informationsfreiheit, sondern auch das Redaktionsgeheimnis.

Der EMGR entschied, dass eine übergeordnete Funktion des klagenden Medienunternehmens darin bestehe die offene Diskussion zu fördern und einschlägige Ideen zu verbreiten. Dies sei durch die Pressefreiheit geschützt. Dem stünde die Offenlegung der Nutzerinformationen entgegen. Die entsprechende Weigerung verfolge das legitime Ziel „den Ruf anderer zu schützen“. Die EMRK sehe „kein absolutes Recht auf Online-Anonymität“ vor. Das Verbergen von Identitäten sei jedoch seit Langem ein Mittel, „um Repressalien oder unerwünschte Aufmerksamkeit zu vermeiden“. Dieses Instrument sei geeignet „den freien Fluss von Meinungen, Ideen und Informationen zu fördern, insbesondere auch im Internet“. Presseorganen müsse es daher möglich sein Anonymität mit eigenen Mitteln wirksam zu verteidigen.

Bei den fraglichen Äußerungen handle es sich weder um Hassrede noch um Aufrufe zur Gewalt, stellt der EGMR klar. Es wäre Aufgabe der nationalen Gerichte gewesen die konkurrierenden Interessen abzuwägen. Sie hätten dies aber nicht getan, wobei insbesondere der OGH nicht einmal Gründe angeführt habe, warum die Belange der Kläger die des Unternehmens an der Geheimhaltung der Identität der Nutzer überwiegen sollten.

Einen Eingriff in das Redaktionsgeheimnis sahen die Straßburger Richter nicht, da die Kommentatoren nicht als journalistische Quellen gelten könnten. Auch einen Anspruch auf Schadenersatz erkannten sie nicht an. Österreich muss dem „Standard“ aber die mit der Klage verknüpften Kosten und Ausla-

gen in Höhe von 17.000 Euro erstatten. Rechtsanwältin Maria Windhager, die das Medienhaus vertrat, bezeichnete das Urteil als „Watsche für den OGH". Es müsse immer zwischen zulässiger politischer Kritik und Hasskommentaren unterschieden werden (Krempl, Kritik in Online-Forum: Menschengerichtshof stärkt Anonymität im Netz, www.heise.de 08.12.2021, Kurzlink: https://heise.de/-6288864).

Conseil d´État

Bußgeld gegen Google wegen Cookie-Intransparenz bestätigt

Der Conseil d'Etat (Staatsrat), das oberste Gericht Frankreichs, bestätigte mit Urteil vom 28.01.2022 die Entscheidung der Datenschutzbehörde CNIL, dass Google wegen undurchsichtiger Cookie-Einstellungen und dem Setzen solcher Browserdateien ohne die erforderliche Zustimmung insgesamt 100 Mio. Euro Strafe zahlen muss (No 449209).

Damit wies der Staatsrat die Argumente Googles gegen die Sanktionsmaßnahme der Commission Nationale de l'Informatique et des Libertés (CNIL) vom Dezember 2020 (DANA 1/2021, 52) zurück und stellte fest, dass der US-Konzern seinen Verpflichtungen zum Einholen einer informierten Einwilligung der User vor dem Setzen von Cookies nicht nachgekommen ist. Die von der CNIL verhängten Geldbußen gegen den Hauptsitz des Unternehmens in Kalifornien und die Europazentrale in Irland sind demnach nicht unverhältnismäßig. Der Staatsrat begründete dies vor allem mit den hohen Gewinnen, die der Suchmaschinenriese mit personalisierter Online-Werbung und den dafür gesammelten Daten erzielt. Das Gericht verwies auf die dominante Position Googles in Frankreich mit einem Marktanteil von über 90% und rund 47 Millionen Usern.

Die CNIL hatte bei einer Kontrolle im März 2020 festgestellt, dass Google sieben Cookies automatisch auf den Computern der Nutzer ablegte, sobald diese auf die Website gelangten. Darunter waren vier entsprechende Browserdateien, die nur Werbezwecken und dem damit verknüpften Tracking dienten. Während der Untersuchung änderte der Konzern zwar seine Praktiken im August 2020, informierte die Nutzer aber weiterhin nicht direkt und ausdrücklich über den Zweck der Cookies und die Möglichkeiten diese abzulehnen.

Die Strafen verhängte die Datenschutzbehörde nicht auf Basis der Datenschutz-Grundverordnung (DSGVO). Sie stützte sich auf Artikel 82 des nationalen Gesetzes über Informatik und Freiheiten, mit dem der französische Gesetzgeber die europäische E-Privacy-Richtlinie von 2002 umgesetzt hatte. Der Conseil d'Etat entschied zudem, dass das in der DSGVO vorgesehene System der einheitlichen Anlaufstelle (One-Stop-Shop) auf das Setzen von Cookies nicht anwendbar sei und wendete primär die nationalen rechtlichen Vorgaben an.

Das erwähnte französische Gesetz war laut der Entscheidung auch deswegen anwendbar und die CNIL für die Durchsetzung zuständig, weil die französische Google-Niederlassung die Cookies ausspielte. Sie musste den Fall daher nicht an die irische Datenschutzbehörde DPC weiterleiten, die nach der DSGVO federführend für den Konzern zuständig ist. Die Kontroll- und Sanktionspraxis der DPC steht wegen ihrer Zurückhaltung massiv in der Kritik (DANA 2/2021, 126 f.). Die Richter urteilten zudem, dass der Ausschluss des One-Stop-Shop-Ansatzes in Bezug auf Cookies klar genug sei. Sie sahen sich daher nicht verpflichtet den Europäischen Gerichtshof um eine Vorentscheidung zu ersuchen. Dies hatte Google mit seiner Klage gegen den CNIL-Beschluss gefordert.

Mit dem Urteil bleibt der Conseil d'Etat seiner bisherigen Linie treu. Schon im Juni 2020 hatte er eine 50-Millionen-Strafe der CNIL gegen Google mitgetragen, die zu ihrer Zeit die höchste auf Grundlage der DSGVO verhängte Sanktion war (DANA 3/2020, 202). Auch dabei ging es um intransparente Datenschutz-Einstelloptionen und personalisierte Werbung ohne ausreichende rechtliche Basis. Erst im Januar 2022 verhängte die CNIL gegen Google erneut wegen Verstoß gegen Artikel 82 des französischen E-Privacy-Gesetzes eine Strafe von insgesamt 150 Millionen Euro. In diesem Fall stellten die Kontrolleure fest, dass Besucher von google.fr und youtube.com öfter klicken mussten, um Cookies abzulehnen als sie anzunehmen (Krempl, Cookie-Einwilligung: Französisches Gericht bestätigt hohe Strafe gegen Google, www.heise.de 29.01.2022, Kurzlink: https://heise.de/-6342543).

BGH

Facebooks Klarnamenpflicht unzulässig

Der Bundesgerichtshof (BGH) hat mit Urteilen vom 27.01.2022 eine Klausel in den Nutzungsbedingungen von Facebook gekippt, wonach ein Nutzer des sog. sozialen Netzwerks grundsätzlich den Namen verwenden muss, den er auch im täglichen Leben gebraucht (Az.: III ZR 3/21 und III ZR 4/21). Die Bestimmung habe die Kläger zum Zeitpunkt ihrer Einbeziehung in den Nutzungsvertrag 2018 „entgegen den Geboten von Treu und Glauben" unangemessen benachteiligt. Der BGH urteilte gemäß der alten Gesetzeslage des bis zum 30.11.2021 gültigen Telemediengesetzes (TMG) und der europäischen Datenschutz-Richtlinie, deren Wirksamkeit seit 25.05.2018 von der Datenschutz-Grundverordnung (DSGVO) abgelöst wurde. Der vorsitzende Richter Ulrich Herrmann wies ausdrücklich darauf hin, dass „die unmittelbare Reichweite unserer Entscheidung auf Altfälle begrenzt" sei.

Gemäß den Urteilen ist die Klausel zur Klarnamenpflicht „nicht klar und verständlich" gewesen. Sie sei von „wesentlichen Grundgedanken" hiesiger Gesetze abgewichen. Eine unangemessene Benachteiligung sei im Zweifel anzunehmen, wenn wesentliche Rechte oder Pflichten, die sich aus der Natur eines Vertrags ergeben, so eingeschränkt werden, „dass die Erreichung des Vertragszwecks gefährdet ist".

Das Oberlandesgericht (OLG) München hatte Facebook mit Urteil vom 08.12.2020 im Recht gesehen und die Sperrung der zwei Nutzenden akzeptiert, die ihr Profil unter Pseudonym geführt hatten (DANA 1/2021, 61). Der BGH hob beide Urteile teilweise auf und verurteilte Facebook beziehungsweise die Konzernmutter Meta im Verfahren

III ZR 3/21 dazu es zu dulden, dass der Kläger seinen Profilnamen in ein Pseudonym ändert. Das Unternehmen muss es dem Kläger ermöglichen die Funktionen seines Kontos unter Pseudonym zu verwenden.

Der BGH stützt sich auf § 13 Abs. 6 des bis zum 30.11.2021 gültigen TMG. Dieser verpflichtete Anbieter die Nutzung ihrer Dienste „anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist“. Das Anfang Dezember 2021 in Kraft getretene Telekommunikations-Telemedien-Datenschutz-Gesetz schreibt diese Vorgabe fort (§ 19 Abs. 2 TTDSG). Facebook sei es zwar nicht zumutbar gewesen die Inanspruchnahme des Netzwerks zu ermöglichen, ohne dass der jeweilige Nutzer zuvor – etwa bei der Registrierung – im Innenverhältnis seinen Klarnamen mitgeteilt hatte. Für die anschließende Verwendung der angebotenen Dienste unter Pseudonym bejahten die Richter dagegen die Zumutbarkeit. Die Klarnamenpflicht falle hier „ersatzlos“ weg.

Im Verfahren III ZR 4/21 verurteilte der BGH Facebook dazu das gesperrte Nutzerkonto der Klägerin freizuschalten und ihr „unbeschränkten Zugriff“ auf die zugehörigen Funktionen zu gewähren. Der Konzern könne von der anderen Partei nicht verlangen ihren Profilnamen in ihren wahren Namen zu ändern. Die Bestimmung zur Klarnamenpflicht in den hier maßgeblichen Nutzungsbedingungen zum Stand 30.01.2015 sei ebenfalls unwirksam. Dies habe das Landgericht Berlin bereits Anfang 2018 in einem Verbandsklageverfahren herausgearbeitet (Az.: 16 O 341/15; DANA 1/2018, 60 f.).

In beiden Verfahren zog der BGH die alte EU-Datenschutzrichtlinie von 1995 heran. Die DSGVO enthält zwar keine ausdrückliche Bestimmung zur anonymen oder pseudonymen Inanspruchnahme von Online-Diensten. Diese neuen Vorgaben sind laut den Karlsruher Richtern aber nicht entscheidend gewesen, weil sie erst seit dem 25.05.2018 gelten. Für die Rechtslage komme es aber „auf den Zeitpunkt der Einbeziehung der jeweiligen Allgemeinen Geschäftsbedingungen in das Vertragsverhältnis an“.

Die BGH-Urteile gelten so zunächst nur für ältere Fälle. Das OLG München hatte argumentiert, die Bundesregierung habe im Streit um die DSGVO auf europäischer Ebene vergeblich versucht ein Recht auf pseudonyme Nutzung in die Verordnung hinein zu verhandeln. Der deutsche Paragraf für Pseudonyme sei daher nun im Sinne des EU-Rechts auszulegen. Für Meta ist die BGH-Ansage ein Rückschlag. Der Konzern hatte sich vorab überzeugt gezeigt, „dass Menschen mehr Verantwortung für ihre Aussagen und Handlungen übernehmen, wenn sie ihren echten Namen auf Facebook verwenden“. Facebook begründete seine Klarnamenpflicht u.a. damit, dass sie helfe Hass und Hetze zu reduzieren. Experten sind sich aber darüber einig, dass es zum Geschäftsmodell des sozialen Netzwerks gehört mehr kontroverse Inhalte an die Nutzer auszuspielen als etwa sachliche Diskussionen. Die Plattform profitiert davon, wenn die Nutzer länger bleiben – und das tun sie eher bei kontroversen Inhalten. Die Gegner einer Pflicht sich mit seinem Klarnamen anzumelden, argumentieren grundsätzlicher: Für sie ist es eine Frage der freiheitlichen Ordnung, ob man sich anonym am Diskurs beteiligen dürfe oder nicht. Wenn Facebook Klarnamen einfordere, verstoße das Unternehmen gegen den allgemeinen Grundsatz der Datensparsamkeit.

Zuletzt hatte sich das EU-Parlament in seiner Position für den geplanten Digital Services Act (DSA) dafür ausgesprochen, dass Betreiber von Online-Plattformen „angemessene Anstrengungen“ unternehmen sollen, um die anonyme Nutzung und Bezahlung von Online-Diensten zu ermöglichen. Das Ampel-Regierungsbündnis setzt auf eine Login-Falle, um Täter zu identifizieren. Dabei sollen vor allem Betreiber sozialer Netzwerke wie Facebook und Twitter gemeinsam mit der Polizei eng zusammenarbeiten, um Verdächtige und deren IP-Adresse zu ermitteln, sobald sie sich erneut einloggen. Ermittler könnten die Internetkennung dann mit Bestandsdaten der Zugangsanbieter abgleichen und so deren Namen und Anschrift erhalten (s.o. S. 26, Martin-Jung, Max Mustemann lebt, SZ 28.01.2022, 18; Krempl, BGH kippt Klarnamenpflicht: Facebook darf Pseudonyme nicht generell untersagen, www.heise.de 27.01.2022, Kurzlink: https://heise.de/-6340626).

VG Wiesbaden

Nutzung des US-Cloud-Dienstes Akamai vorläufig gestoppt

Das Verwaltungsgericht (VG) Wiesbaden hat in einem Eilverfahren entschieden, dass die staatliche Hochschule RheinMain den Dienst Cookiebot nicht länger auf ihrer Webseite www.hs-rm.de einbinden darf (Az. 6 L 738/21.WI). Der Cookiebot bittet Nutzer um Einwilligung in die Speicherung von Cookies auf ihrem Endgerät, über die Daten der Webseiten-Besucher auf Server eines US-Unternehmens übertragen werden.

Ein Nutzer, der sich im Online-Katalog der Bibliothek der Hochschule regelmäßig nach Fachliteratur erkundigte, hatte damit erfolgreich einen Unterlassungsantrag gestellt. Er monierte, dass der Einwilligungsmanager des dänischen Anbieters Cybot Daten wie seine IP-Adresse auf einen Server des in den USA ansässigen Cloud-Unternehmens Akamai Technologies übermittle. Selbst wenn sich der entsprechende Server möglicherweise in der EU befinde, habe der US-Konzern Zugriff darauf, sodass der US-amerikanische Cloud Act mit breiten Abfragemöglichkeiten für US-Behörden greife.

Diese Argumentation wurde von der zuständigen Kammer des VG mit drei Richtern geteilt: Da sich Akamais Zentrale im US-Bundesstaat Massachusetts befindet, führe der Cookiebot zu einer nach der Datenschutz-Grundverordnung (DSGVO) unzulässigen Übermittlung. Akamai unterliege dem Cloud Act, der US-Diensteanbieter dazu verpflichtet „sämtliche in ihrem Besitz, Gewahrsam oder ihrer Kontrolle“ befindlichen Daten offenzulegen, unabhängig vom Speicherort. Mit Blick auf die Schrems-II-Entscheidung des Europäischen Gerichtshofs (EuGH) vom 16.07.2020 sei diese Praxis unzulässig (vgl. DANA 3/2020, 199 ff.). Der Cookiebot bitte Nutzer nicht um Einwilligung zu einem Transfer persönlicher Informationen in die USA, und unterrichte sie nicht über die damit verbundenen Risiken. Verantwortlich für die unmittelbar ausgelöste Erhebung und den Transfer an Akamai sei die Hochschule.

Mit der Entscheidung hat sich – soweit ersichtlich – erstmals ein deutsches Gericht mit dem Verhältnis zwischen dem Cloud Act und der DSGVO befasst. Es folgte dabei einschlägigen Ausführungen des Europäischen Datenschutzausschusses (EDSA) zum Schrems-II-Urteil, mit dem der EuGH das Abkommen für den Privacy Shield zum Datentransfer in die USA gekippt hat. Die Richter sehen eine rechtfertigungsbedürftige Datenübertragung bereits, wenn die Konzernmutter eines Cloud-Anbieters in den USA sitzt. Dies ist nicht nur bei Akamai der Fall, sondern auch bei anderen Cloud-Größen wie Amazon, Microsoft, Google, Apple und Cloudflare. Sollte der Beschluss im Hauptverfahren bestätigt und in der Folge rechtskräftig werden, dürfte er weit über die Hochschule und den Cookiebot hinaus wirken.

Die Bildungseinrichtung hatte sich auf eine Standardvertragsklausel, die zwischen Cybot und Akamai abgeschlossen worden sein soll, berufen. An Cybot werde nur die „anonymisierte" Internetkennung (letzte drei Ziffern auf Null gesetzt), Datum und Uhrzeit der Zustimmung, Nutzeragent des Browsers, die URL, ein anonymer, zufälliger und verschlüsselter Schlüssel sowie der Einwilligungsstatus übermittelt, meinte die Hochschule. Soweit für den Verbindungsaufbau zu den Servern eine ungekürzte IP-Adresse an Akamai übertragen werde, werde diese nicht verarbeitet oder gespeichert.

Der Antragsteller hielt dagegen, dass durch den Akamai-Server offenkundig Klardaten verarbeitet würden. Es könne sich höchstens um eine Transportverschlüsselung handeln. Eine solche stelle keine ausreichende Schutzmaßnahme im Sinne der Schrems-II-Entscheidung dar. Diese Ansicht wurde von einem Sachverständigen des Hessischen Datenschutzbeauftragten bestätigt.

Das Gericht verwies auf eine Erklärung Cybots, wonach die IP-Adresse nicht anonymisiert werde. Selbst wenn der Cookie-Dienst nur bei einmaligem Laden die ungekürzte Internetkennung übertrage, handle es sich schon um eine „datenschutzrechtlich beachtliche Verarbeitung" eines personenbezogenen Datums. Der „anonyme" Schlüssel schließe eine „Individualisierung" anhand der übrigen Daten nicht aus. Der Nutzer könne identifiziert werden, auch wenn sein Name nicht bekannt sei. Damit handle es sich um ein personenbeziehbares Datum. Eine endgültige Regelung bleibt dem Hauptverfahren vorbehalten.

Jonas Breyer, Rechtsanwalt des Antragstellers, nannte die Entscheidung „spektakulär". Ein unzulässiger Datentransfer liege damit auch bei Webseiten-Plugins vor, die von einem Cloud-Dienst mit US-Bezug gehostet und geladen werden. Dies betreffe nicht zuletzt Werkzeuge Sozialer Netzwerke, Google Analytics, reCAPTCHA oder YouTube, US-Videokonferenzdienste sowie andere Online-Funktionen von US-Anbietern.

Das VG stelle klar, dass der Personenbezug von Cookies immer im Kontext weiterer, meist umfangreich vorliegender Daten zu beurteilen sei. Zuvor habe der EuGH ausgeführt, dass für eine rechtmäßige Übertragung in die USA Standardvertragsklauseln um geeignete zusätzliche technische und organisatorische Maßnahmen wie Verschlüsselung ergänzt werden müssten. Die gängigen US-Anbieter verzichten bisher in der Regel auf solche Absicherungen. Ihre Dienste seien daher, so der Anwalt „regelmäßig nicht rechtskonform nutzbar". Rechtlich seien sogar Arbeitgeber verantwortlich, die ihre Beschäftigten mit einschlägigen Diensten hantieren lassen. Als mögliche Lösung sieht Breyer – neben durchgehender Verschlüsselung – Treuhandansätze, wie sie Microsoft mit T-Systems ausprobiert habe und Google auflegen wolle (Krempl, Gericht: Deutsche Webseiten dürfen keine US-Cookies setzen, www.heise.de 08.12.2021, Kurzlink: https://heise.de/-6288818).

Buchbesprechungen



Buchner, Benedikt (Hrsg.)
Datenschutz im Gesundheitswesen Grundlagenwissen – Praxislösungen – Entscheidungshilfen
Loseblatt incl. 27. Nachtragslieferung, November 2021
AOK-Verlag Remagen,
ISBN 978-3-553-430000-5

(tw) Das Gesundheitswesen ist einer der Sektoren, in denen derzeit die Praxis wie Regulierung der Datenverarbeitung besonders dramatische Entwicklungen durchmacht. Krankenhäuser sind Opfer von Ransomware-Angriffen; Ex-Gesundheitsminister Spahn brachte ein Gesetz nach dem anderen durch die letzte Legislaturperiode. Das von Benedikt Buchner herausgegebene Loseblattwerk ist darauf angelegt diese aktuellen Entwicklungen nachzuzeichnen. Nachdem das Werk seine Kinderkrankheiten (DANA 2/2012, 98) abgelegt hat, deckte die Informations- und Materialsammlung schon vor einigen Jahren tatsächlich alle Bereiche des Gesundheitswesens ab mit seinen vielen Verästelungen, etwa dem Internet- oder dem Informationssicherheitsrecht (DANA 3/2017, 181). Das Werk ist auch Grundlage für eine – reduzierte – gebundene Ausgabe für Leute, die sich in diesen Bereich einarbeiten wollen (DANA 2/2018, 122 u. 2/2019, 114).

Derweil wird die inzwischen vollständige Abdeckung des Gesundheitsbereichs durch Neubearbeitungen in der Loseblattsammlung sukzessive auf einen neuen Stand gebracht, so nun jüngst der Krankenhaussektor durch die bei der Landesdatenschutzbeauftragten Bremen tätige Maren Pollmann, zuvor zur

Datenschutzorganisation (Kapitel B), zu den rechtlichen Grundlagen (Kapitel A, bearbeitet durch den Herausgeber) oder zur IT-Sicherheit. Die Texte wurden umfassend an die DSGVO angepasst.

Richtete sich das Ursprungswerk noch stark an den Praktiker, der keine Notwendigkeit sieht, durch weitergehende Literatur die Erkenntnisse zu vertiefen, so enthalten die Texte zunehmend Referenzen zu weitergehenden Quellen. Dies ist bei dieser komplexen Materie auch nötig. Diese Angaben werden aber nur sehr gezielt und sparsam eingesetzt, so dass Irritationen über Darstellungen juristischer Streitstände u.Ä. vermieden werden und der Blick aufs Wesentliche gewahrt bleibt. Durch Darstellungen spezifischer Fallgestaltungen, von Urteilen und Aufsichtsbehördenpositionen, Hilfen und Verweisen wird die an der Praxis ausgerichtete Grundtendenz unterstrichen.

Für den Praktiker ist die Loseblattsammlung dadurch eine gute Grundlage und zugleich Fundgrube. Wegen der separaten Darstellung einzelner Anwendungsbereiche durch unterschiedliche Autorinnen und Autoren ließ es sich offenbar nicht vermeiden, dass es in den einzelnen Kapiteln zu Redundanzen kommt. Dies hat zwangsläufig zur Folge, dass die Übersichtlichkeit bei einzelnen Fragestellungen leidet und man unter Umständen zu einer Fragestellung Auskünfte an mehreren Stellen suchen muss und auch finden wird.

Dadurch leidet aber der Nutzen nicht. Ein auch in der aktuellsten Nachlieferung mitgesendeter Index hilft bei der Suche. Praktikern, insbesondere Datenschutzbeauftragten, ist das Werk warm zu empfehlen.

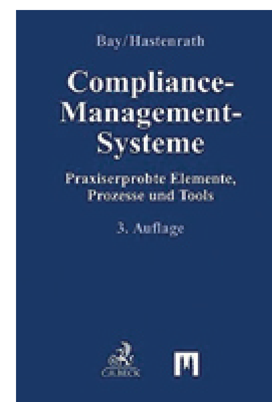
Polizeirecht – Entgrenzung und Protest
Bürgerrechte & Polizei/CILIP 127 (Dezember 2021)
ISSN 0932-5409

(ha) Schon seit 1978 gibt es den Informationsdienst „Bürgerrechte & Polizei“, dessen damaliges Ziel es war „sich nicht nur mit wissenschaftlichen Methoden den ‚Apparaten Innerer Sicherheit‘ zu widmen, … sondern zugleich Daten und Dokumente … für die Öffentlichkeit dauerhaft zugänglich zu machen“ (S. 4). Dieser Aufgabe kommt der „Newsletter on civil liberties & police“ (CILIP) heute immer noch nach. Auch in der aktuellen Ausgabe veröffentlicht CILIP (S. 70 ff.) die Liste der 15 polizeilichen Todesschüsse in 2020 mit je einer kurzen Fallbeschreibung. Die Todesschüsse werden von dem Berliner Journalisten Otto Diederichs eingeordnet in die Zahlen der gesamten offiziellen Schusswaffengebrauchsstatistik der deutschen Polizeibehörden und ergänzt um kurze Stellungnahmen, wie beispielsweise die zur Zunahme der unbeabsichtigten Schussabgaben. „Deren Zahl stieg von 11 im Jahr 2018 über 56 in 2019 auf nunmehr 98 im vergangenen Jahr. Da läuft etwas schief!“ (S. 71). Die seit 1976 von CILIP gesammelten Daten über tödliche Polizeischüsse wurden jetzt – so der Beitrag von Johannes Filter und Matthias Monroy – neu sortiert und auf der Webseite https://polizeischuesse.cilip.de dargestellt: „Mit unserer neuen Übersicht können wir die These stützen, dass eine beträchtliche Zahl von psychisch beeinträchtigten Menschen Opfer von Polizeischüssen werden.“ (S. 77)

Insgesamt widmet sich das aktuelle Heft 127 allerdings schwerpunktmäßig der Polizeipolitik der Bundesländer in den letzten fünf Jahren. Dazu richten Eric Töpfer und Marius Kühne den Fokus auf die Verschärfungen des Polizeirechts, mit dem von Bayern über Hessen und Rheinland-Pfalz bis Mecklenburg-Vorpommern neue Befugnisse eingeführt wurden. Bereits bestehende Befugnisse wie Videoüberwachung und Schleierfahndung wurden erweitert und die Waffenkataloge beispielsweise um Taser ergänzt. Der Beitrag ordnet die Entwicklung ein und schließt mit den Worten: „Wer erwartet, dass im Gegenzug zur Ausweitung polizeilicher Kompetenzen wirksame Mechanismen zur Kontrolle der Anwendung dieser Befugnisse geschaffen würden, wird enttäuscht.“ (S. 16)

Hier können nicht alle Beiträge aufgeführt werden, so dass nur darauf hingewiesen sei, dass weitere Artikel eine „Bilanz der Proteste gegen verschärfte Polizeigesetze“ (S. 17 ff.) ziehen und die Erfolge der Mobilisierung gegen das Bayerische Polizeiaufgabengesetz (S. 34 ff.) bewerten. Der Staats- und Verwaltungsrechts-Professor Clemens Arzt schließlich analysiert die Umsetzung der europäischen JI-Richtlinie in deutsches Polizeirecht (S. 43 ff.); die Fachanwältin Anna Busl widmet sich der Problematik von „Gefährdern“ und der Politikwissenschaftler Florian Krahmer betrachtet „Gefährliche Orte und die Definitionsmacht der Polizeibehörden“.

Das CILIP-Heft 127 enthält (wieder) Artikel für Artikel spannende und teils wütend machende Fakten und Analysen aus dem Bereich „Bürgerrechte und Polizei“. Die Lektüre wird den Leserinnen und Lesern dieser Zeitschrift dringend empfohlen!



Bay, Karl-Christian; Hastenrath, Katharina (Hrsg.)
Compliance-Management-Systeme. Praxiserprobte Elemente, Prozesse und Tools
3. neu bearb. Aufl., Verlag C.H.Beck, München 2022; 318 S., 79,- €; Teil der Reihe: Compliance für die Praxis.
ISBN 978 3 406 88018 0

(hdn) Die Autoren dieses Werkes, einschließlich der Herausgeber, stammen aus der Wissenschaft und aus der Praxis des Compliance-Managements. Dem Praxisbezug wird hohes Gewicht beigemessen. Zielgruppe sind Compliance-Verantwortliche des Mittelstands und der Großunternehmen. Die Inhaltsübersicht umfasst bis auf ein Abbildungsverzeichnis alle wesentlichen Merkmale eines wissenschaftlichen Ansprüchen genügenden Buches.

Die Gliederung orientiert sich weitgehend an den Komponenten des IDW PS 980 sowie den ISO-Compliance-Standards und beinhaltet in den mit Paragrafen nummerierten Kapiteln die Themen

- Compliance-Kultur, in dem auf die Unternehmenskultur als Basis der Compliance-Kultur hingewiesen wird, die sich durchaus auch mal an den Unternehmenszielen „reiben" kann und z. B. auch Begriffe wie Diversität oder Change Management umfasst;

- Compliance-Ziele, die idealerweise in den Unternehmenszielen eingebettet sein und deren Abweichung ggf. sanktioniert werden sollte;

- Compliance-Risiken, das als eines der umfassenderen Kapitel die Maßnahmen von der Risiko-Identifikation über deren Bewertung hin zu Risikosteuerung und Berichterstattung beinhaltet;

- Compliance-Programm, in dem auch auf die aktuelle Gesetzeslage (VerSanG-E, Whistleblower-Richtlinie) eingegangen wird und eine Vielzahl von grafisch hervorgehobenen Beispielen angeboten werden; in diesem recht umfassenden Kapitel (40 S.) widmet sich die Autorin auch dem Thema Digitalisierung und der Homeoffice-Problematik;

- Compliance-Organisation, in dem von der organisatorischen Gestaltung bis zur Besetzung des Compliance-Verantwortlichen alle wesentlichen Einrichtungen und Regelungen behandelt werden;

- Compliance-Kommunikation, das als eines der wichtigsten Themen auch das umfassendste Kapitel darstellt und in dem die logisch aufgebauten Kommunikationsphasen detailliert beschrieben und unter anderem deren Alternativen mit ihren Vor- und Nachteilen aufgezeigt werden. Interessierte finden hier einen Vorschlag zur Entwicklung eines eigenen Compliance-Videoclips.

Die letzten vier Kapitel widmen sich der Überwachung und Verbesserung, der Effektivität der Compliance-Management-Systeme, deren Relevanz und last but not least dem Status Quo der Compliance aus Sicht der Wirtschaftsprüfer. Auf die Compliance von Datenschutzgesetzen geht das Werk nicht dediziert ein.

In allen Kapiteln wird intensiv auf die jeweiligen Komponenten der Compliance eingegangen, wobei, und das macht der Werk sehr wertvoll, mit praxisnahen Vorschlägen an die jeweiligen Lösungen herangegangen wird. Besonders in den Kapiteln über die Programme zur Compliance und zur Kommunikation wird sehr eingehend die praktische Umsetzbarkeit veranschaulicht. Hilfreiche Abbildungen, Tabellen, Übersichten finden sich im gesamten Buch.

Als Nicht-Jurist habe ich das Buch gern und mit Interesse gelesen. Die Autoren verzichten wohltuend auf die sonst üblichen juristischen Begriffskompositionen. Das Werk kann man daher durchaus als Hand- und Lehrbuch verstehen; tatsächlich wird es auch in der Lehre eingesetzt.

Cartoon





Bild: Lucas Cranach der Ältere – Paradies, https://commons.wikimedia.org/w/index.php?curid=9819597, gemeinfrei